ID: 740246
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:01:20
Date: 07/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

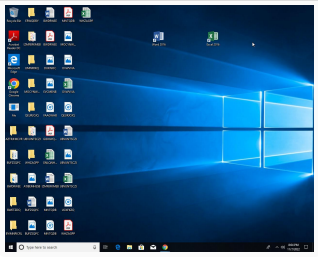
Windows Analysis Report

file.exe

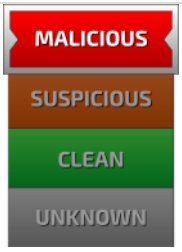
Overview

General Information

Sample Name:	file.exe
Analysis ID:	740246
MD5:	76b726f03046fc4..
SHA1:	3f1dec6167f3e52..
SHA256:	983b19f3d65f374.
Tags:	exe
Infos:	



Detection



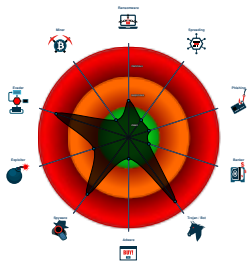
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- Connects to many ports of the same…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queries sensitive video device infor…
- Contains functionality to inject code…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5840 cmdline: C:\Users\user\Desktop\file.exe MD5: 76B726F03046FC48FCC93701C14A3894)
  - conhost.exe (PID: 4720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 100032 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
  - WerFault.exe (PID: 100204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5840 -s 947 48 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4408 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5840 -s 947 48 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "194.110.203.100:32796"
  ],
  "Bot Id": "711",
  "Message": "License Not Found",
  "Authorization Header": "24e3340d853c89cad1e25194559ee778"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.298695211.0000000000A23000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000000.295452062.0000000000A23000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.312912092.0000000000A23000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.256237407.0000000000892000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.358247423.0000000007453000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.9f0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.file.exe.9f0000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x2529c:$s5: delete[] • 0x529f0:$pat14: , CommandLine: • 0x4a6db:$v2_1: ListOfProcesses • 0x4a46f:$v4_3: base64str • 0x4b4fa:$v4_4: stringKey • 0x48088:$v4_5: BytesToStringConverted • 0x470f0:$v4_6: FromBase64 • 0x4885c:$v4_8: procName • 0x48bdf:$v5_1: DownloadAndExecuteUpdate • 0x4a37f:$v5_2: ITaskProcessor • 0x48bcd:$v5_3: CommandLineUpdate • 0x48bbe:$v5_4: DownloadUpdate • 0x49273:$v5_5: FileScanning • 0x483f7:$v5_7: RecordHeaderField • 0x47e16:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.3.file.exe.890000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.file.exe.890000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x21070:$pat14: , CommandLine: • 0x18d5b:$v2_1: ListOfProcesses • 0x18aef:$v4_3: base64str • 0x19b7a:$v4_4: stringKey • 0x16708:$v4_5: BytesToStringConverted • 0x15770:$v4_6: FromBase64 • 0x16edc:$v4_8: procName • 0x1725f:$v5_1: DownloadAndExecuteUpdate • 0x189ff:$v5_2: ITaskProcessor • 0x1724d:$v5_3: CommandLineUpdate • 0x1723e:$v5_4: DownloadUpdate • 0x178f3:$v5_5: FileScanning • 0x16a77:$v5_7: RecordHeaderField • 0x16496:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.file.exe.a22780.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.6 - Destination IP: 194.110.203.100

Timestamp:	192.168.2.6194.110.203.10049721327962850027 11/07/22-20:02:48.733611
SID:	2850027

Source Port:	49721
Destination Port:	32796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 194.110.203.100 - Destination IP: 192.168.2.6	−
Timestamp:	194.110.203.100192.168.2.632796497212850353 11/07/22-20:02:51.076682
SID:	2850353
Source Port:	32796
Destination Port:	49721
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.6 - Destination IP: 194.110.203.100	−
Timestamp:	192.168.2.6194.110.203.10049721327962850286 11/07/22-20:03:07.287990
SID:	2850286
Source Port:	49721
Destination Port:	32796
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

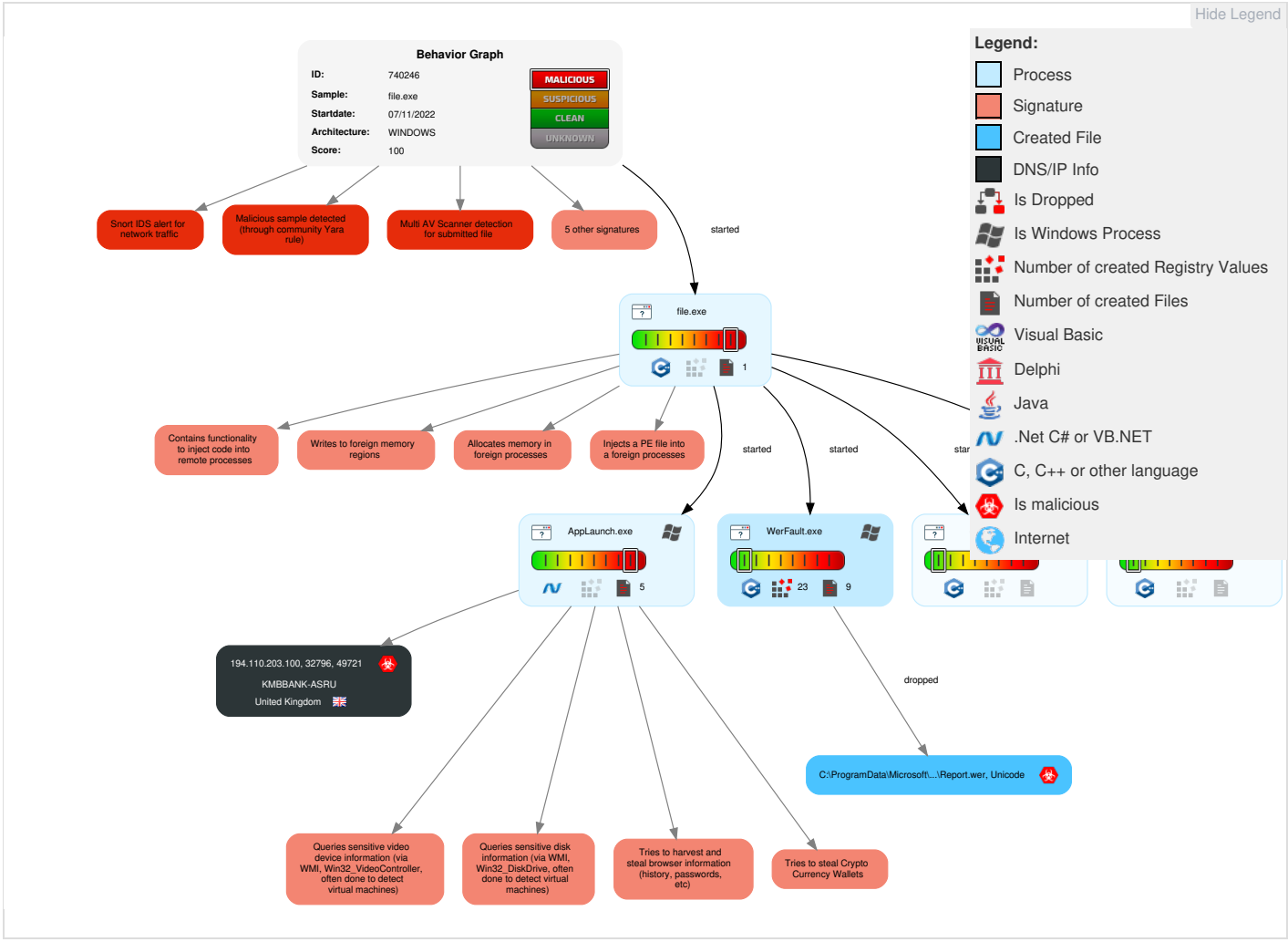
Remote Access Functionality

Yara detected RedLine Stealer

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	2 2 1 Windows Management Instrumentation	Path Interception	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	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	1 Input Capture	2 5 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	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 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Process Discovery	SMB/Windows Admin Shares	3 Data from Local System	Automated Exfiltration	1 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)	4 1 1 Process Injection	NTDS	2 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window 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	3 1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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	Compile After Delivery	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 4 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

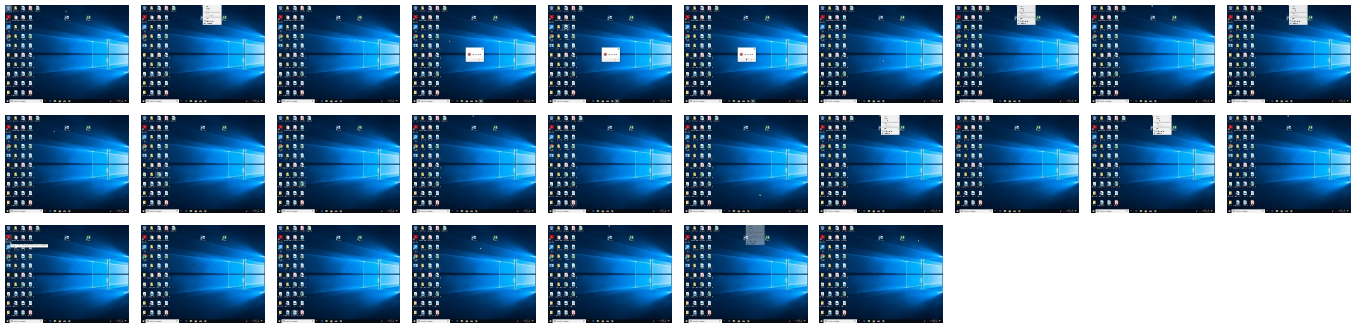
Behavior Graph



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	35%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000002.00000002.3724089 78.0000000008599000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372136186.000000000853800 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371455315.000 000000843C000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.373051767.0000000008690000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.371778582 .00000000084BA000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372805407.000000000862F000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.37318 8331.00000000086AD000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.371644889.000000000849D 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371355743.0 00000000841F000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.372688030.0000000008612000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3592862 93.0000000007569000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372551259.00000000085B600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.359831862.000 00000075F5000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.360602784.0000000007682000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.358674223 .00000000074DD000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372032571.000000000851B000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000002.00000002.3725512 59.00000000085B6000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.359831862.00000000075F500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.360602784.000 0000007682000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.358674223.00000000074DD000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.372032571 .000000000851B000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.363059245.000000000775200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.363059245.000000000775200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faulth	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000002.00000002.3606846 78.000000000768F000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.363059245.000 0000007752000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.363059245.000000000775200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high

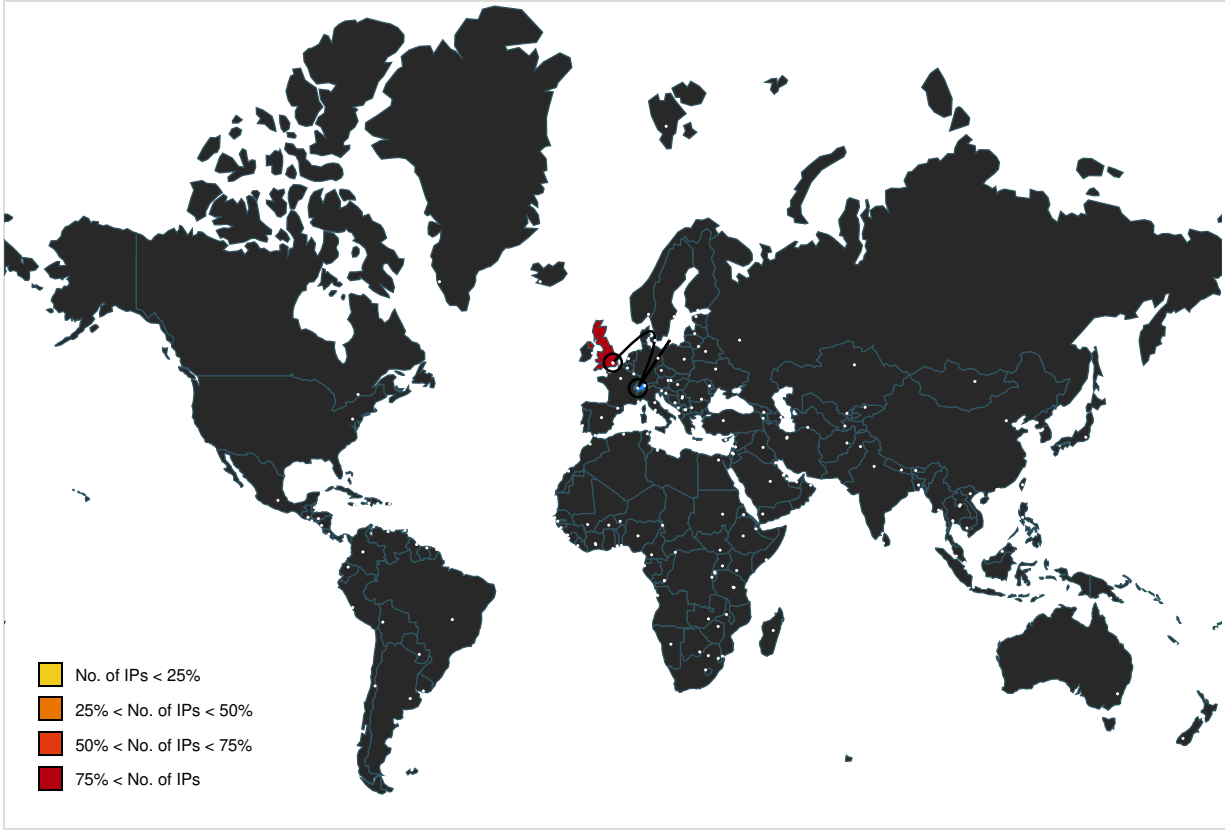
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000002.00000002.3606846 78.000000000768F000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	file.exe, file.exe, 00000000.00000000.298695211.00 00000000A23000.00000004.00000001.0100000 0.00000003.sdmp, AppLaunch.exe, 00000002 .00000002.358247423.0000000007453000.000 00004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000002.00000002.3606846 78.000000000768F000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000002.00000002.3725512 59.00000000085B6000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.359831862.00000000075F500 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.360602784.000 0000007682000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.358674223.00000000074DD000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.372032571 .000000000851B000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	AppLaunch.exe, 00000002.00000002.3724089 78.0000000008599000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372136186.000000000853800 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371455315.000 000000843C000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.373051767.0000000008690000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.371778582 .00000000084BA000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372805407.000000000862F000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.37318 8331.00000000086AD000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.371644889.000000000849D 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371355743.0 00000000841F000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.372688030.0000000008612000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3592862 93.0000000007569000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372551259.00000000085B600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.359831862.000 00000075F5000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.360602784.0000000007682000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.358674223 .00000000074DD000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372032571.000000000851B000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000002.00000002.3606846 78.000000000768F000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoor dinationContextResponse	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Can cel	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000002.00000002.3606846 78.000000000768F000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.357962850.00000000073C100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.363059245.000 0000007752000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token- profile-1.1#SAMLV2.0	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token- profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2004/04/security/trust/RST/S CT	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2006/02/addressingidentity	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/envelope/	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	AppLaunch.exe, 00000002.00000002.3724089 78.0000000008599000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372136186.000000000853800 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371455315.000 000000843C000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.373051767.0000000008690000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.371778582 .00000000084BA000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372805407.000000000862F000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.37318 8331.00000000086AD000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.371644889.000000000849D 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.371355743.0 00000000841F000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.372688030.0000000008612000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3592862 93.0000000007569000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.372551259.00000000085B600 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.359831862.000 00000075F5000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.360602784.0000000007682000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.358674223 .00000000074DD000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.372032571.000000000851B000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id23Response	AppLaunch.exe, 00000002.00000002.3630592 45.0000000007752000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	AppLaunch.exe, 00000002.00000002.3582474 23.0000000007453000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	AppLaunch.exe, 00000002.00000002.3579628 50.00000000073C1000.00000004.00000800.00 020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.110.203.100	unknown	United Kingdom		42693	KMBBANK-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	740246
Start date and time:	2022-11-07 20:01:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
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:	15
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:	mal100.troj.spyw.evad.winEXE@8/6@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 97.3% (good quality ratio 90.8%) • Quality average: 78.1% • Quality standard deviation: 29.1%

HCA Information:	• Successful, ratio: 100% • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com
- Execution Graph export aborted for target AppLaunch.exe, PID 100032 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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 NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:02:46	API Interceptor	1x Sleep call for process: WerFault.exe modified
20:03:04	API Interceptor	26x Sleep call for process: AppLaunch.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_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c\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):	0.6146576752327751

Encrypted:	false
SSDEEP:	192:8x8bPvcWkHBUZMXz03jE/u7sLS274ItmhB:NCBUZMXYjE/u7sLX4ItA
MD5:	87FC08DFB1CDBBEECED61F71782858B6
SHA1:	D8DE7FFC4D42D45D576DF967B761A3E9C612A0C8
SHA-256:	36E068F5844B4955F152E6259DF99FABE9F93FC9B750B5715F306B7776E358B2
SHA-512:	28528648875BBCF03372726817FF71836E63C641B0C2AE6FC6A56B9D1C2C83C941CC0FF158083DFECE0AB22F4917CA76D3A1206E93F770CE8BFA85B1CF3AB1(5
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.2.3.5.3.7.6.2.6.2.1.5.1.9.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.1.2.3.5.3.7.6.4.8.2.4.6.3.8.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.5.e.5.5.b.a.3.-.f.4.5.b.-.4.4.9.a.-.9.b.7.7.-.f.7.3.c.e. 3.0.b.8.7.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.=.d.4.0.f.e.9.2.b.-.9.f.1.8.-.4.4.b.5.-.b.9.a.8.-.5.1.2.d.8.8.3.0.1.e.1.4.....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.=.0.0.0.0.1.6.d.0.-.0.0.0.1.-.0.0.1.a.-.4.3.0.f.-.0.c.e.4.2.6.f.3.d.8.0.1.....T.a.r.g.e.t.A.p.p.I. d.=.W.:.0.0.0.6.7.e.4.9.2.d.7.6.8.e.7.9.7.3.1.6.2.4.b.c.d.f.2.e.7.6.1.5.f.9.1.8.0.0.0.0.f.f.f.f.!.0.0.0.0.3.f.1.d.e.c.6.1.6.7.f.3.e.5.2.c.4.a.7.2.3.0.9.5.b.f.f.9.9.9.a.e.d.3.1.c.7. 1.c.3.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2./.1.1.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Nov 8 04:02:43 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	2326066
Entropy (8bit):	2.72014094231897
Encrypted:	false
SSDEEP:	6144:XOBvoBDGxNDw128unr2TkWcgviLt5OTl4MRkifkOJn19DoEWp5:XCopEl5aVccHlvt19DoEWf
MD5:	C6E94E8DC885B44B7491FB58D0DDC0A8
SHA1:	7A723B25DB742C0F6D819498D1E46826E5D4BFC4
SHA-256:	1B04E24A87AC1013804FC3C020491B7A5B3AF44126264646468FF327DABD4364
SHA-512:	9776267A59359E97EFFB32D98F4290B961CAAF2C2F50AAA35DC7F4D08928AAFEC94297C932AC4DF96AAF0C5FBF4E7C1C55F08D0F4C75B83B8E241CF64E53B9 37
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....ic.....4..... ...<.....T.....T.....8.....T.....g..z.....\.....H.....U.....B.....GenuineIn telW.....T.....ic.....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\WERE7E1.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):	8268
Entropy (8bit):	3.693331909547304
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLCE6Dh6YqbSUVZ0igmfBSVS/OCprV89bWbsfNym:RrlsNit6F6YGSUjJgmfOScWgfp
MD5:	9A2D91907082D657F924A56CD80E3F64
SHA1:	31DA20E5E800B1EA2C3A4803E3CB2DCFEFE9AEEC
SHA-256:	CD54AEB84D9F2D772C98904CE0F24F0387EE722D9548D45B08A75C2831C591F4
SHA-512:	245BEDDB7C37623166424A1EA5D5DF20F55AF927C9251C6473BBA8528F0090512680DDCE1876C284EEBD2DD01A6DD6440481BE6473793E3BA75F5F3B9075BBF A
Malicious:	false
Reputation:	low
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.>.5.8.4. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4521

Entropy (8bit):	4.423660373002552
Encrypted:	false
SSDEEP:	48:cvIwSD8zswJgtWI9FBWgc8sqYjP8fm8M4JhOFi+q8aBtdfNwd:uITf2yQgrsqYwJLhtlNwd
MD5:	7B0C03096324CD48C67D527D0204126D
SHA1:	6E3986447CF7AB690A5E6ABCCE08B110FDFF7F13
SHA-256:	325FFFF9B3CFCDA929C98430A946C0D4703C27D3169040296957226BA8D162F6
SHA-512:	8A15EA240D7A20FC8BF9E3D298B4D4DC307E4CD0A4C0DE207A05F004A700D1E9C4815A311923E4283B475423939528229B5C0A56AD672F0A8C885644968CA32
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="1770553" />.. <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\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHKx1qHje:iqXeqm00YqhQnouOqLqdqNq2qzcGtlxU
MD5:	75BC6DB42CE4C37482926043D9B80BC9
SHA1:	700BDF1D18804FBE60EB0318B290C37CDC60EA41
SHA-256:	15F15BDEB42AD40DBCB6BB9064C33B51CB43EDB99820EDE647350BE604AAF58A
SHA-512:	26E15E546BBD6518265BAC343F952E75B30C7927143D293780F456A5B44C1E1B6B7D074DF00BC6328D23E52FE9E3F8850A879B129C35F47B0ED864E9C640BA4F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

\Device\ConDrv

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:gQdcXW:gQn
MD5:	5F702714045C206E93012159054928D0
SHA1:	3AEF30FD196AE230CD4C194006A3185524EFC82A
SHA-256:	A6706758CED31780EA9392DDDFE62CF54D9D03EED69FCCBB00234AF431892043
SHA-512:	AC25D23590C1907E726362F5C752022A0EC7F1D5E10B7A6CEB500CB6A685AACC2B5A8340EFB4AE0B30B186A17395BB7C682151F2389D765F1F890842B588466
Malicious:	false
Preview:	76587687123

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.233138744312905
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:	355328
MD5:	76b726f03046fc48fcc93701c14a3894
SHA1:	3f1dec6167f3e52c4a723095bff999aed31c71c3
SHA256:	983b19f3d65f37400eeb404fd838e322041fc26335ed14e08d29addbb87fcea9
SHA512:	82adb5bb73b094bc71179b8273d1b4cfcd58562edb396bf0aa029b70098ba982a5a7d8a4edf179400523afba8d275c1ddffcbdf061a833545f1ce4d31aa12f8a
SSDEEP:	6144:Sy1R2biwZ3RIcq5KIVwOTi4bBI8UAOdJYJfPfc+freo5JSjZY85U:Sy1RqiwZ3RIcq5d/knL5zr
TLSH:	F474CF40B5D3DA72D8B3543609E0DB75897DB8200F705AFF67E4476B4E202C3A9B2A79
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... J..sJ..sJ..s^..rG..s^..r...s^..r\..s...r[..s...r^..s...r...s^..rI..sJ..s...s...rK..s...rK..sRichJ..s.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x408d22
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x636954D1 [Mon Nov 7 18:56:17 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e2a07bb4b81e6c6d0f72670722ee7e56

Entrypoint Preview

Instruction
call 00007F7774ABC519h
jmp 00007F7774ABBFC9h
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007F7774ABC16Bh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007F7774ABC15Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]

Instruction
cmp ecx, eax
jc 00007F7774ABC15Eh
add edx, 28h
cmp edx, esi
jne 00007F7774ABC13Ch
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007F7774ABC14Bh
push esi
call 00007F7774ABC9C5h
test eax, eax
je 00007F7774ABC172h
mov eax, dword ptr fs:[00000018h]
mov esi, 00455E2Ch
mov edx, dword ptr [eax+04h]
jmp 00007F7774ABC156h
cmp edx, eax
je 00007F7774ABC162h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007F7774ABC142h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007F7774ABC159h
mov byte ptr [00455E30h], 00000001h
call 00007F7774ABC7B3h
call 00007F7774ABE9E7h
test al, al
jne 00007F7774ABC156h
xor al, al
pop ebp
ret
call 00007F7774AC67B2h
test al, al
jne 00007F7774ABC15Ch
push 00000000h
call 00007F7774ABE9EEh
pop ecx
jmp 00007F7774ABC13Bh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
cmp byte ptr [00455E31h], 00000000h
je 00007F7774ABC156h
mov al, 01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3185c	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x57000	0x1c58	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2fe0c	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2fe28	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x13c	.rdata
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	0x22d22	0x22e00	False	0.5762768817204301	data	6.6605774583744495	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0xdf72	0xe000	False	0.5242222377232143	data	5.554648741907312	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x24930	0x23c00	False	0.7996271306818182	data	7.495127080621036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x57000	0x1c58	0x1e00	False	0.7291666666666666	data	6.3994808113416175	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetCurrentProcess, CreateThread, GetModuleHandleA, GetProcAddress, MultiByteToWideChar, FreeConsole, CreateFileW, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, LCMapStringEx, GetStringTypeW, GetCPInfo, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, TerminateProcess, RaiseException, RtlUnwind, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, HeapAlloc, HeapFree, GetFileType, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, CloseHandle, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, GetProcessHeap, HeapSize, WriteConsoleW

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6194.110.203.100497213279628500271 1/07/22-20:02:48.733611	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49721	32796	192.168.2.6	194.110.203.100
194.110.203.100192.168.2.632796497212850353 11/07/22-20:02:51.076682	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	32796	49721	194.110.203.100	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6194.110.203.1 0049721327962850286 11/07/22- 20:03:07.287990	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49721	32796	192.168.2.6	194.110.203.100

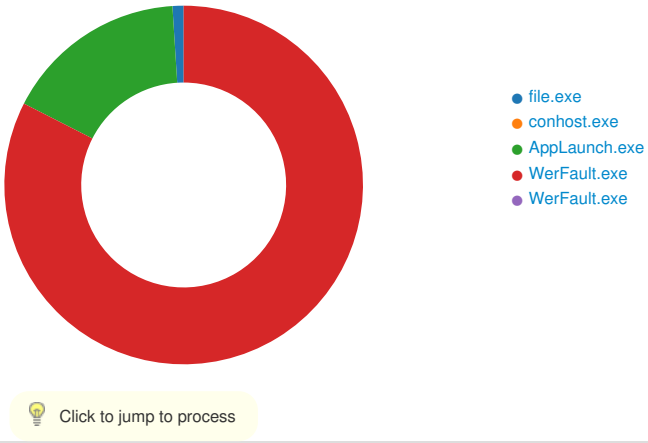
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 7, 2022 20:02:48.070909023 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:02:48.119203091 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:02:48.119393110 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:02:48.733611107 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:02:48.782188892 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:02:48.870331049 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:02:51.028397083 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:02:51.076682091 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:02:51.181005001 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:01.529644966 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:01.595479012 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:01.595535994 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:01.595587015 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:01.595690012 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:01.650660038 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:03.444371939 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:03.494756937 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:03.519723892 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:03.568541050 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:03.619524002 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.190699100 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.240565062 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:05.291585922 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.463870049 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.512433052 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:05.557214022 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.610408068 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.658844948 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:05.713537931 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.787441969 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.835834026 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:05.850558996 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.898813963 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:05.917280912 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:05.967777014 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.010380983 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.177527905 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.226139069 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.227144957 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.276046991 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.652749062 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.701364040 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.702847958 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.752557039 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.771147013 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.819082022 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.869879961 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.944365978 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:06.992187977 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:06.992892981 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.041780949 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.084103107 CET	49721	32796	192.168.2.6	194.110.203.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 7, 2022 20:03:07.132455111 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.138436079 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.187535048 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.190057993 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.238189936 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.239080906 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.287101984 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.287990093 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.337461948 CET	32796	49721	194.110.203.100	192.168.2.6
Nov 7, 2022 20:03:07.385507107 CET	49721	32796	192.168.2.6	194.110.203.100
Nov 7, 2022 20:03:07.485074043 CET	49721	32796	192.168.2.6	194.110.203.100

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **5840**, Parent PID: **3452**

General

Target ID:	0
Start time:	20:02:16
Start date:	07/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x9f0000
File size:	355328 bytes
MD5 hash:	76B726F03046FC48FCC93701C14A3894
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000000.298695211.0000000000A23000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000000.295452062.0000000000A23000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.312912092.0000000000A23000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.256237407.0000000000892000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	36	6	success or wait	11	A07DC5	WriteFile
unknown	unknown	48			invalid handle	1	A07DC5	WriteFile
unknown	unknown	48			object type mismatch	126	A07DC5	WriteFile
unknown	unknown	1			object type mismatch	10	A07DC5	WriteFile

Analysis Process: conhost.exe PID: **4720**, Parent PID: **5840**

General

Target ID:	1
Start time:	20:02:16
Start date:	07/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **100032**, Parent PID: **5840**

General

Target ID:	2
Start time:	20:02:21
Start date:	07/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x10d0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.358247423.0000000007453000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.358247423.0000000007453000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.363059245.0000000007752000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Reputation:	high

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	6D62CF06	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	6D62CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C47BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C47BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D93C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	0	2843	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6D93C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D60CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	7	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6C471B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	8	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	12	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	324	end of file	2	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C471B4F	ReadFile

Analysis Process: WerFault.exe PID: **100204**, Parent PID: **5840**

General

Target ID:	4
Start time:	20:02:34
Start date:	07/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5840 -s 94748
Imagebase:	0x1030000
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	6A6E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A6D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp.xml	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2C96.tmp.csv	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CD5.tmp.txt	success or wait	1	6A6D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	0	32	4d 44 4d 50 fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 69 63 fd 05 12 00 00 00 00 00	MDMP ic	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.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 0b 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 54 05 00 00 fd 03 00 00 fd 16 00 00 fd fd 69 63 00 00 00 00 04 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 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTic0Pacific Standard TimePacific Daylight Time	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	3184	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 20 06 fd 00 fd fd 52 77 00 04 00 00 fd 68 fd fd 00 00 00 00 00 00 00 00 54 fd 75 00 06 5e fd 00 23 00 00 00 fd 02 01 00 0c fd 75 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++ RwhTu^#u+	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1620	168	24 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 06 5e fd 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 70 0c 00 00	$^p	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	4616	20	05 00 00 00 fd fd 75 00 00 00 00 00 74 12 00 00 5c 12 00 00	ut\	success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	4700	4724	fd fd fd 77 fd 1a 54 77 fd fd fd fd fd fd 75 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 18 72 01 00 14 72 01 00 fd fd fd fd 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 30 50 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	wTwurr$0Pu	success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	11112	4096	10 fd 75 00 00 00 76 00 00 fd 75 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 60 50 00 00 00 00 00 fd 16 00 00 24 17 00 00 00 00 00 00 2c 60 50 00 00 30 50 00 7a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	uvu`P$,`P0Pzpw	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	3900	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 20 fd 75 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 75 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++ uw#u+	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1792	48	24 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 60 50 00 00 00 00 00 fd fd 75 00 00 00 00 00 74 12 00 00 5c 12 00 00 fd 02 00 00 3c 0f 00 00	$ `Put\<	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	3046	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	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	2288	752	00 00 fd 73 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd 54 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 47 54 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 fd fd 1a 00 00 00 00 00 48 37 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 16 fd 05 00 00 00 00	sQTBB?$@AZb 0#GTH7@	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	15208	524288	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 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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	539496	524288	00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd fd 00 00 03 00 00 00 09 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd fd 00 00 03 00 00 00 09 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 00 fd 00 00 03 00 00 00 09 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 04 fd 00 00 03 00 00 00 09 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00	Thread Thread Thread Thread Thread	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1063784	318242	01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd 30 01 00 03 00 00 00 08 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd 30 01 00 03 00 00 00 08 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd 30 01 00 03 00 00 00 08 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd 30 01 00 03 00 00 00 08 00 00 00 00 00 00 00 0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 00 00 00 00 00 20 00 00 fd 16 00 00 fd 30 01	0Thread 0Thread 0Thread 0Thread 0	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	1382026	944040	04 00 00 00 00 00 00 00 68 3b 00 00 00 00 00 00 00 00 00 00 03 00 1f 00 02 00 00 00 fd fd 00 00 78 3b 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 00 00 00 00 00 03 00 1f 00 02 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 00 00 00 00 00 fd 00 0f 00 02 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 fd 3b 00 00 00 00 00 00 00 00 00 00 02 00 10 00 02 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 10 3c 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 1c 00 00 00 00 00 00 00 3e 3c 00 00 00 00 00 00	h;x;;;;;<><	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0DB.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 08 12 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 67 0e 00 7a 16 15 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <TT8Tgz\H	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5840</Pid>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 36 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>27692</Uptime>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1308	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1426	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 31 00 32 00 36 00 32 00 34 00 31 00 39 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>1262419968</PeakVirtualSize>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1516	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1520	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1526	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 31 00 33 00 33 00 30 00 37 00 39 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>13307904</VirtualSize>	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1606	78	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 31 00 37 00 38 00 36 00 35 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>178651</PageFaultCount>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1694	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 35 00 33 00 36 00 36 00 35 00 32 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>25366528</PeakWorkingSetSize>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1802	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 33 00 36 00 32 00 39 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>3629056</WorkingSetSize>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 34 00 30 00 36 00 31 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 50 00 61 00 67 00 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>406120</QuotaPeakPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 34 00 30 00 35 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>405952</QuotaPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2124	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 36 00 32 00 34 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 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>262400</QuotaPeakNonPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2260	106	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 39 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>9512</QuotaNonPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2376	74	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 37 00 35 00 37 00 37 00 36 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>757760</PagefileUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2460	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 36 00 39 00 32 00 32 00 36 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>69226496</PeakPagefileUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2564	70	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 37 00 35 00 37 00 37 00 36 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>757760</PrivateUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 32 00 34 00 35 00 35 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3924554</Uptime>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 34 00 38 00 39 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>64890</PageFaultCount>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 33 00 33 00 31 00 32 00 38 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>133128192</PeakWorkingSetSize>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 33 00 32 00 36 00 36 00 39 00 34 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>132669440</WorkingSetSize>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 31 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>1121904</QuotaPeakPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 37 00 30 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>1070104</QuotaPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4024	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>90184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>79912</QuotaNonPagedPoolUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 35 00 35 00 36 00 37 00 32 00 38 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>55672832</PagefileUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 35 00 35 00 38 00 31 00 36 00 31 00 39 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>55816192</PeakPagefileUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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 35 00 35 00 36 00 37 00 32 00 38 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>55672832</PrivateUsage>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4808	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 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>APPCRASH</EventType>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	4878	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	8	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5458	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5462	2	09 00		success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5464	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5504	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5508	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5510	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5548	4	0d 00 0a 00		success or wait	6	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5552	2	09 00		success or wait	12	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	5556	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6110	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6114	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6116	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6156	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6160	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6162	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6200	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6204	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6208	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6302	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6306	2	09 00		success or wait	2	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6310	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 6a 00 6e 00 70 00 79 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>bjnpye, Inc.</SystemManufacturer>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6416	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6420	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6424	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 6a 00 6e 00 70 00 79 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>bjnpye7,1</SystemProductName>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6520	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6524	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6528	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6648	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6652	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6656	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 32 00 39 00 31 00 39 00 39 00 31 00 39 00 34 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>1629199194</OSInstallDate>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6738	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6742	2	09 00		success or wait	2	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6746	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6848	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6852	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6856	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6924	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6928	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6930	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6970	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6974	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	6976	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7010	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7014	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7018	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7120	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	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7156	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7160	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7162	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7186	4	0d 00 0a 00		success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7190	2	09 00		success or wait	6	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7194	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7442	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7446	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7448	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7474	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7478	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7480	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 31 00 2d 00 30 00 38 00 54 00 30 00 34 00 3a 00 30 00 32 00 3a 00 34 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-08T04:02:44Z">	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7580	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7584	2	09 00		success or wait	2	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7588	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 32 00 39 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 38 00 34 00 30 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 34 00 38 00 39 00 30 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 34 00 38 00 39 00 30 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="299" PID="5840" UptimeMS="4890" TimeSinceCreationMS="4890" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7858	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7878	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7882	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7884	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7928	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	7974	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 35 00 65 00 35 00 35 00 62 00 61 00 33 00 2d 00 66 00 34 00 35 00 62 00 2d 00 34 00 34 00 39 00 61 00 2d 00 39 00 62 00 37 00 37 00 2d 00 66 00 37 00 33 00 63 00 65 00 33 00 30 00 62 00 38 00 37 00 61 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d5e55ba3-f45b-449a-9b77-f73ce30b87a7</Guid>	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8072	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8076	2	09 00		success or wait	2	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8080	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 31 00 2d 00 30 00 38 00 54 00 30 00 34 00 3a 00 30 00 32 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>2022-11-08T04:02 :44Z</CreationTime>	success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8184	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE7E1.tmp.WERInternalMetadata.xml	8228	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8AD.tmp.xml	0	4521	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	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c\Report.wer	0	2	fd fd		success or wait	1	6A6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c\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	130	6A6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2badc22553de5577b078ab10208ce43d7e4f5c0_ae08e2d3_8757f04c\Report.wer	7242	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 31 00 33 00 35 00 32 00 35 00 32 00 38 00	MetadataHash=-61352528	success or wait	1	6A6D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	success or wait	1	6A6F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6A6F1FB2	RegCreateKeyExW
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A6D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	ProgramId	unicode	00067e492d768e79731624bcdf2e7615f9180000ffff	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	FileId	unicode	00003f1dec6167f3e52c4a723095bff999aed31c71c3	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	LowerCaseLongPath	unicode	c:\users\user\desktop\file.exe	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	LongPathHash	unicode	file.exe|92928141	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	Name	unicode	file.exe	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	Publisher	unicode		success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	Version	unicode		success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	BinFileVersion	unicode		success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	BinaryType	unicode	pe32_i386	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	ProductName	unicode		success or wait	1	6A6F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	ProductVersion	unicode		success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	LinkDate	unicode	11/07/2022 18:56:17	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	BinProductVersion	unicode		success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	Size	B	00 6C 05 00 00 00 00 00	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	Language	dword	0	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	IsPeFile	dword	1	success or wait	1	6A6F36BF	unknown
\REGISTRY\A\{ca2ede7b-eeae-5fe1-ec8a-e8fb9d03cbee}\Root\InventoryApplicationFile\file.exe|92928141	IsOsComponent	dword	0	success or wait	1	6A6F36BF	unknown
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 06 5E 9F 00 02 00 00 00 00 00 00 00 FC FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6A6F1FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **4408**, Parent PID: **5840**

General

Target ID:	6
Start time:	20:02:42
Start date:	07/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5840 -s 94748
Imagebase:	0x1030000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly