ID: 628111
Sample Name:
62835e34e60c1.dll
Cookbook: default.jbs
Time: 10:56:45
Date: 17/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

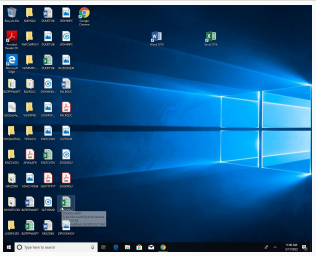
Windows Analysis Report

62835e34e60c1.dll

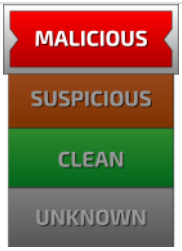
Overview

General Information

Sample Name:	62835e34e60c1.dll
Analysis ID:	628111
MD5:	5572213d17be7d.
SHA1:	5e8b27d57f6c9d..
SHA256:	f58f9c8e6a62223..
Tags:	DHL dll gozi isfb italy ursnif
Infos:	



Detection



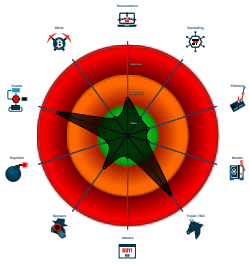
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Writes registry values via WMI
- Uses 32bit PE files
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7012 cmdline: loaddll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7064 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7120 cmdline: rundll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 1448 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 400 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6480 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 408 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3272 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 436 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"uFHdIp1dwWhvkEA2yTiBbeuMW6YDB1lsKD5xr+wbKQpSTgCxKW/AXnU7L/HiYIBOAaOvelJb2/pY2jRw/FTeNeGEktAn4DWXMKOPXXT0NA64cjWTlmZ01c3ZQu3caOM/Vp3zMRoE3uvOCFkw5pB9m5AVXCHf7c66rMBTCpzNlB06TLav
0Zslv7QoNXagpBRObC3w6aRV9zoEMPsKo8dDtjcXrpjT3cmo/nK2BeLeCRHw4m+Z1wNt/QFKG0JSvLN7KWGp2TqLTGCk8sWmJopJGBcCeH8dEEcUduFFgdi8Cilu/K4cd0diqylW1QdRW2VJSAgt/TyNLQ8XGjESLVVFp5dI5rtAU8yov
Xe+vZ9IsF8=",
  "c2_domain": [
    "config.edge.skype.com",
    "185.189.151.28",
    "185.189.151.70"
  ],
  "botnet": "3000",
  "server": "50",
  "serpent_key": "noA8W2qeaw7z6wk9",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.409022533.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.408311834.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.409143246.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.408868417.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.408399417.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.cb0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.49e94a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.400000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.49e94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 13.107.43.16 −

Timestamp:	192.168.2.513.107.43.1649772802033203 05/17/22-10:46:47.467879
SID:	2033203
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

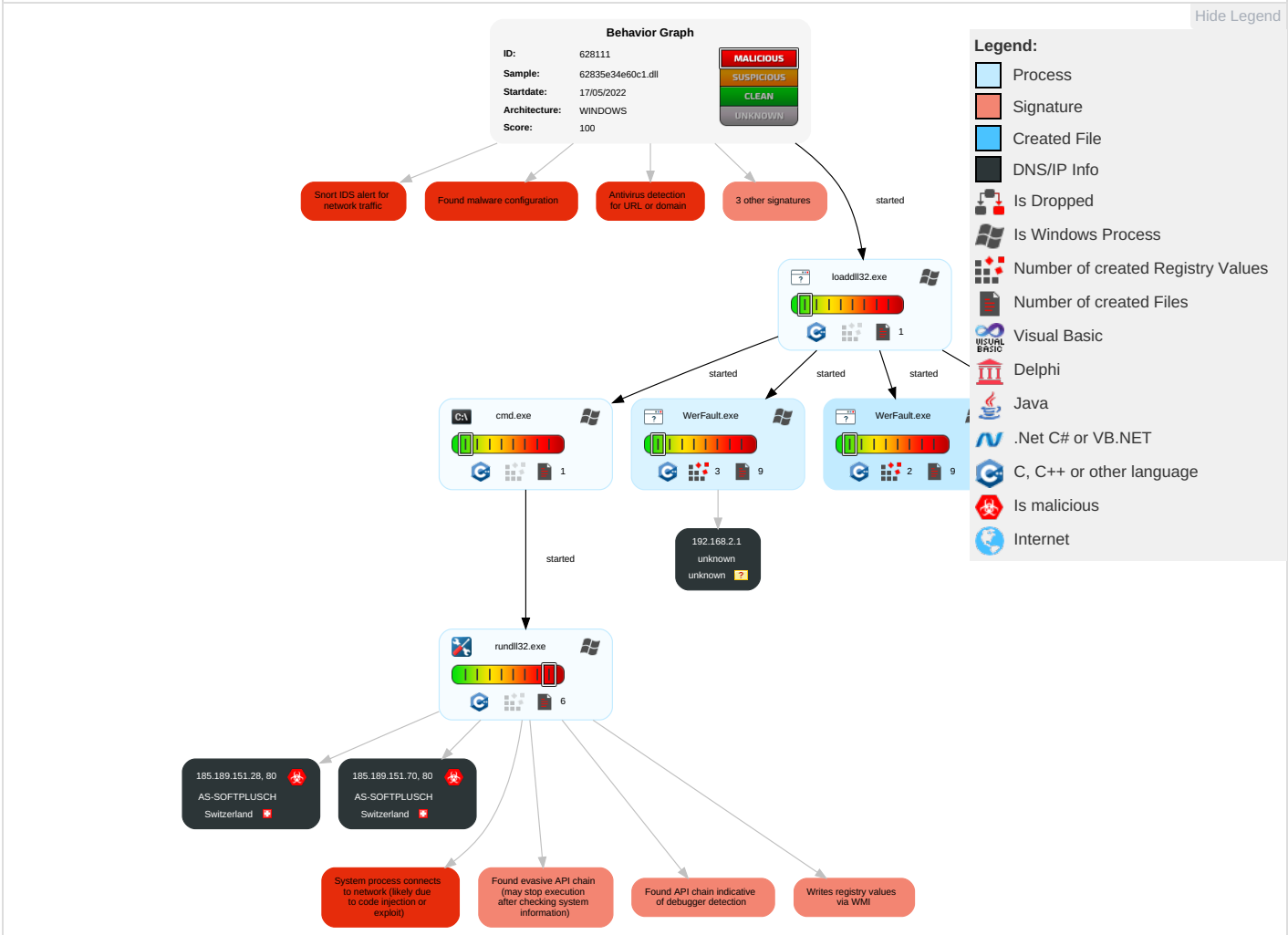
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	1 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	Software Packing	LSA Secrets	1 Process 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	Steganography	Cached Domain Credentials	1 Account 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 System Owner/User 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 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 1 4 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

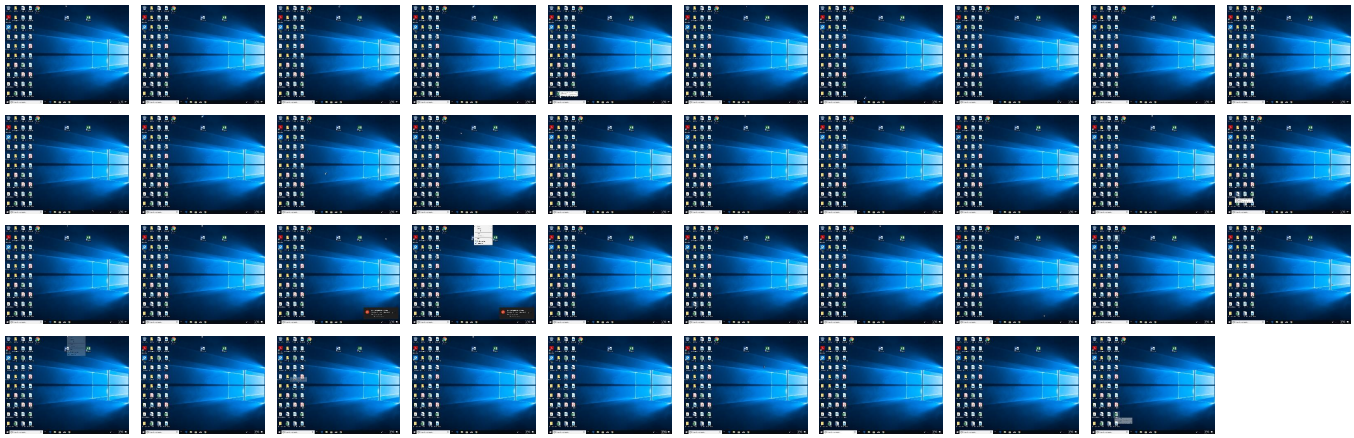
Behavior Graph



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
62835e34e60c1.dll	28%	Virustotal		Browse
62835e34e60c1.dll	29%	ReversingLabs	Win32.Trojan.Generic	
62835e34e60c1.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.cb0000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.189.151.70/drew/aaJEUlLh_/2FLHWWSII4z5Zv8IHOi1/CMWvnEAIAbago4IEJQ4/RXWAE	100%	Avira URL Cloud	malware	

Domains and IPs

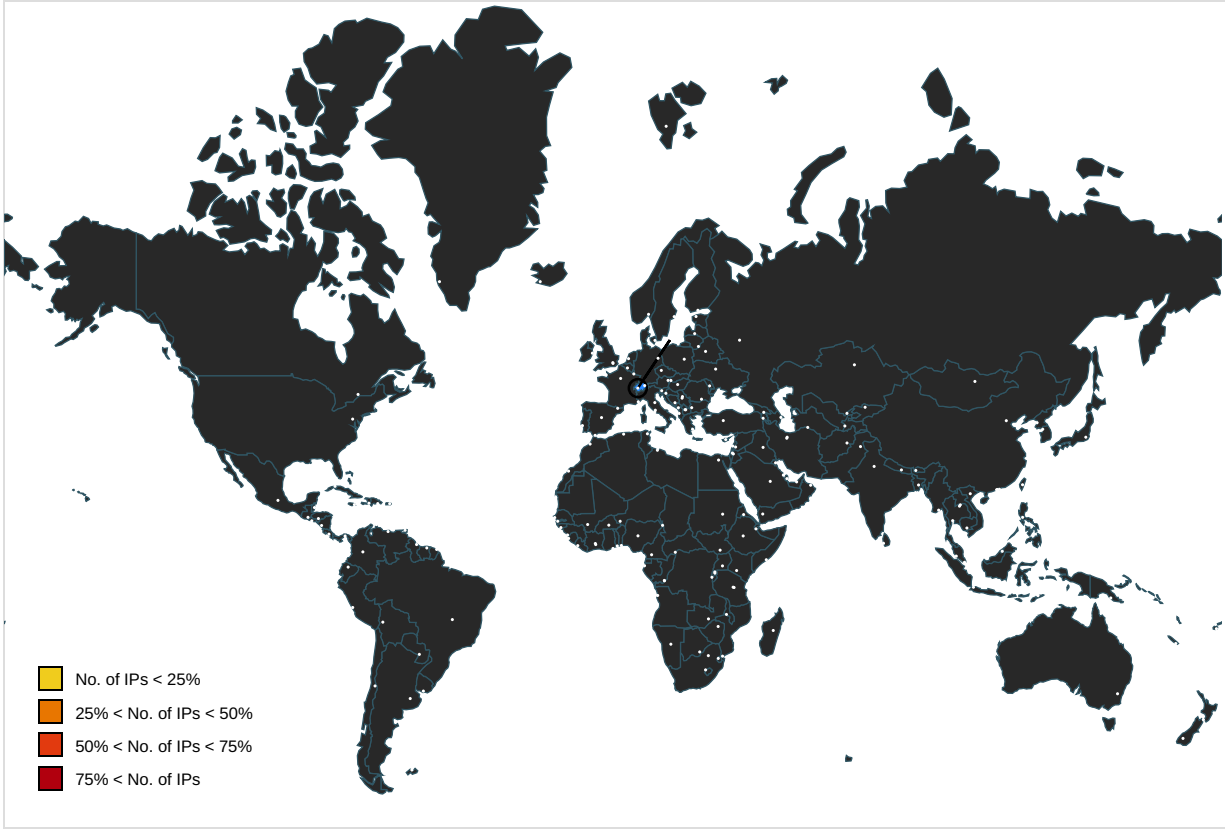
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.189.151.70/drew/aaJEUlLh_/2FLHWWSII4z5Zv8IHOi1/CMWvnEAIAbago4IEJQ4/RXWAE	rundll32.exe, 00000003.00000002.768863780.000000000452B000.00000004.00000010.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.189.151.70	unknown	Switzerland		51395	AS-SOFTPLUSCH	true
185.189.151.28	unknown	Switzerland		51395	AS-SOFTPLUSCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	628111
Start date and time: 17/05/202210:56:45	2022-05-17 10:56:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	62835e34e60c1.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	26
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.evad.winDLL@8/12@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 47.3% (good quality ratio 43.8%) • Quality average: 78.7% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.107.42.16, 20.42.73.29, 104.208.16.94, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7459414164550618
Encrypted:	false
SSDEEP:	96:M5fFbpI8nYy3y9hayCjmfIpXIQcQOgc6OIcEkcw3Ck+a+z+HbHgbVG4rmMXL9iVH:ApiknJHn1Orj4q/u7svS274ItW
MD5:	765ABBA6C1660E911C54330A7BC1606F
SHA1:	E3376463E7F382EC0C345788F105D15C30BC2987
SHA-256:	C408348921E14A33A4213937A6E97F7C6D0455E8092E5BF88F0CD8EDD8C4B60C
SHA-512:	35E23E8F51666B6D37A83BE1ED82EEAE9694E2BBD45A29BE6A765E7F10E266D821D44F406BDBD146E338978EE1FCA9D79E1B78AD0B81FD8D2C350C629FB95D26
Malicious:	false
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.=.1.3.2.9.7.2.8.3.9.0.6.2.2.5.2.5.7.4.....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.=.1.3.2.9.7.2.8.3.9.1.5.6.7.8.3.5.5.5.....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.=.6.7.3.3.9.f.3.5.-.7.3.8.9.-.4.b.f.2.-.b.9.b.a.-.2.7.c.0.a.c.4.d.7.0.6.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.f.b.8.1.5.f.6.-.a.e.5.9.-.4.e.4.b.-.9.b.a.b.-.f.a.5.b.8.7.4.1.7.8.4.2.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.6.4.-.0.0.0.1.-.0.0.1.8.-.0.7.7.3.-.a.d.a.3.1.7.6.a.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7493456943059427
Encrypted:	false
SSDEEP:	96:deWFMI8nYyby9haot7JnxpXIQcQac6pcEccw35+a+z+HbHgbVG4rmMXL9iVff9oO:jpkncH0tGtj4q/u7svS274ItW
MD5:	7D5CDADEA445D9FC80F3C13462755C58
SHA1:	0801623B83DCF91DEFF26BF39AFC4356CB62C2E7
SHA-256:	655C3E14724676AD2FB212AA4B58FAB14CFFB44B9549B560AB1F05F3D1D5855C
SHA-512:	FD575CC9EC555B93190C7EEF30E31363CE9C3A1CE4E2F7BFA77AD91EFEDDBB93963B0EBB745ACBD2615C71C70656915835D279509FE4FAD376670097E415334E
Malicious:	false
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.=.1.3.2.9.7.2.8.3.8.9.5.7.6.4.1.2.7.5.....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.=.1.3.2.9.7.2.8.3.9.0.1.8.1.0.9.8.9.4.....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.=.8.6.8.0.6.f.7.a.-.2.9.9.2.-.4.7.9.b.-.a.6.d.e.-.e.6.1.8.7.0.7.8.f.7.9.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.6.d.0.0.e.f.c.-.4.2.0.a.-.4.9.3.0.-.b.6.4.8.-.8.3.0.8.9.6.a.2.8.1.7.4.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.6.4.-.0.0.0.1.-.0.0.1.8.-.0.7.7.3.-.a.d.a.3.1.7.6.a.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.742784995343186
Encrypted:	false
SSDEEP:	96:XBVI8nYyMy9hayCj+kSZpXIQcQac6pcEccw35+a+z+HbHgbVG4rmMXL9iVff9oUN:xWkn1H0tGtj4q/u7sUS274Itb
MD5:	C3EDDDA902C0A9EB58F7A8088BBC0654
SHA1:	6235DF8E9B1704627AF3CD10857399394ADBBF5F
SHA-256:	7EBA5EEB36AB7086F59A397DF3E4FDF32085CEC5F3929858648A0673DC550119
SHA-512:	563FD41B72D13E28600F38B2D8DC172E08532436F43D56A9DBA919BF3ED1B9387C3673818313B0716E21E99F6CB6C329C37697D3839EC037677478F4B1086FD2
Malicious:	false

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.2.8.3.8.8.3.8.7.4.5.4.1.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.6.8.f.f.9.1.f.-.7.e.4.3.-.4.8.1.7.-.8.0.1.a.-.4.2.0.7.d.7.0.6.1.0.f.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.d.c.1.8.6.d.6.-.a.7.c.2.-.4.e.5.6.-.a.9.2.0.-.b.5.9.5.8.5.3.5.3.c.4.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.6.4.-.0.0.0.1.-.0.0.1.8.-.0.7.7.3.-.a.d.a.3.1.7.6.a.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	3.6913930970467996
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+164PH6Yf9SUWH4gmfZSyo/TCpDh89byLsfWGm:RrlsNiE6uH6YVSUWH4gmfZSPyQfu
MD5:	E8BC5D3AF4FF0FE23D838738B13F56F9
SHA1:	6A924900D3833090E57DDE40B0CD4B7EBA650D60
SHA-256:	2741B81315AB5E1DB21A0AE15AB78AC2D9F3770B440DA330AF145EE624034744
SHA-512:	7D1DE823D290726DDB8471ED60930F3C4753402303BA16CB331500296ADED4B19F7C7D6B592474B588E637BB73A287B3B576B03329B13C02BBB16686762AD9A3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4564
Entropy (8bit):	4.429145263681937
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9DrWgc8sqYjL8fm8M4J2+EXFWwh+q84Pv3JMKcQIcQw0Ld:uITfKAagrsqYEJGQ2L3aKkw0Ld
MD5:	61AE258A83B79F03B5D4686B81BF3C78
SHA1:	C10E2BA375AAE565073FBF01F6A119FBEDF026BC
SHA-256:	CA4FB2889B03A7E961E0A1612A5973326AB83F3CC4DBE7843CA03BFAFEF95ABC
SHA-512:	6ECF08C81D944972DE5FF08F590AAA312F7897AC74ECE5B92C308DF8AD1D02F18660040E814F86F89684381760C37BE67C12F6960F1B2DE47AB61597FDCC9AC
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="1519389" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 17:58:04 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34166
Entropy (8bit):	2.1035543431161714
Encrypted:	false
SSDEEP:	192:vvH3NdZ1zOs2ihEzmXe9qK9Rw8+M3DkhWj:nfqsYGK//PG
MD5:	321951AD431A22ECB02EC4C832337B0F
SHA1:	899351B6A09EAAB03C6530421F8FBA9E8D404ABC
SHA-256:	670CE2681CA71E7DC314175F0BC65E67B0D3D166BD27895B3E947D432B91E8F6
SHA-512:	ED51901C528CC6C3B34ED598B906AE0CEAB14752FEAC869BB1943375BB6B0EA23B4997F3DAFC939FDDE60D321693EB2EB692AD710F9200D0DC53C80315D40ED
Malicious:	false

Preview:	MDMP..... .....,b.....L.....$.....!.....`.....8.....T.....(...Nu.....U.....B..... ..GenuineIntelW.....T.....d...%.b.....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\WERB73.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 17:58:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	46970
Entropy (8bit):	2.3221277094345067
Encrypted:	false
SSDEEP:	192:dW4HNd5z+OsglOGRS4oWl/9HTPHgr+bmWnhEzpXe9qW9a566ZrugozGA3+:r5s8d441B7NbmfZWQW5+
MD5:	BAD8D6ECD0F042F5983B68752F3A24E6
SHA1:	F5BD68A8FA65BF71E2611E035C98148BA2340518
SHA-256:	B7E0DEA36E791094438C940D435A2AF06CDD7A1F456A0F2F9F4EB6536F16BD3B
SHA-512:	2FD7275CFC63A62FC779213AE991172728B3F3E1A8744D8160A3087699BB76B08BC283F0DE5B8F67B0ADA0E55E3B44259EFBAF05239512DF0CE4FCAB590A46D4
Malicious:	false
Preview:	MDMP..... .....B.b.....L.....$.....!.....`.....8.....T.....z.....U.....B..... ..GenuineIntelW.....T.....d...%.b.....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\WERBBBE.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8350
Entropy (8bit):	3.686646157743096
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+H6G86YfzSU8igmf2Sno/TCpNd89b1j1flKnm:RrlsNi+6G86YbSU8igmf2Sw1RfJ
MD5:	00F02820FA5568092CDDA377BEDE9E8B
SHA1:	D2FDCEC39887814BA0066857D0F49A0C6FD52086
SHA-256:	82C2D7DE8D4A309D18F6F8A79DAAACF86F0CBC25E6925CF8709B35C6999BFB5D
SHA-512:	9D93367B52E7BC241B41AFF85F2DCA91E49E64A295E062ABF0EEE8C79D287A312C64E360A67CC5AAE27133582D884CC55DBEB31A12E047E555C364981C7A78D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4665
Entropy (8bit):	4.416373864582268
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPAiJgtWI9DrWgc8sqYj48fm8M4J2+IkFY2m+q8vQ+IyJMKcQIcQw0Kd:uITfNAagrsqYBJi52mKkyaKkw0Kd
MD5:	1335CE8EDCDBDFE5A328FAF185FF5A01
SHA1:	DA1A80FB00F6779880E5288D7AF626524940878D
SHA-256:	A3CB996D41C8D306D585F0341A1196C21D66C21F2A3397087602F476C6FA7489
SHA-512:	0ADBA7B788F7FE0D02C5F606BCABA535D6DB5CE69F9D5619AF12F272D1EBBB60699C6C271B834C1A01A08C2E70BCBD6F2D13DB09D3421C1439DB000BF27028C5
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="1519388" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 17:58:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	33966
Entropy (8bit):	2.0439214950087936
Encrypted:	false
SSDEEP:	192:LQyNdHV7OsuhEzuXebqL9+3/9Wvk75C9yW1AYef:90sfwLEP4c
MD5:	102E4EC10D7F33243C895BDBB8871D5B
SHA1:	222F72EA0B61B9B144450C6E1D77E280920F8463
SHA-256:	9801DF46E16FF2617F44FFAE37CF38B434E6C0597F49EAC4E163E2076336B6B1
SHA-512:	B86E207FC9B691870615ABE6B54660E9914468485C19AE123A8CC13C6210ED03AECDE6315C6339E26A99381E993C9905F7C0CB043832A359AC75C7444006B678
Malicious:	false
Preview:	MDMP..... .....8.b.....L.....$.....!.....`.....8.....T.....(....t.....U.....B..... ..GenuineIntelW.....T.....d...%.b.....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\WERE908.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8338
Entropy (8bit):	3.6985279071998045
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+I6Ak6YfySUjbgmfWSno/TCprD89bGLsfxCm:RrlsNiJ6Ak6YqSUjbgmfWS4GQfV
MD5:	6998C94DAD75CFD4AE57B64851BFEE5A
SHA1:	DDC4E1A9FD39F46DA4E7BC8EAEAB9CEDD7B7275C
SHA-256:	FA08358DE1023D4778B0D08CEC9BE6C670645A93DCDCC3C73DF31EDA02DDF9CF
SHA-512:	5771D2D02EFCB51E39A8B803958078F7872025F0C85311DE08EF5EAB4DA7BF385BF35F4428089DA63048C1090D5A6270DD3632D45DF49EDC5775BDAA4D31ED9 4
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.1. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.46788112177361
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPAiJgtWI9DrWgc8sqYje8fm8M4J2+pZFdFW8+q8490ZJMKcQIcQw0Ld:uITfNAagrsqY/JX3PeZaKkw0Ld
MD5:	9B741B1FF771D0D7427B36E6630DB971
SHA1:	6A359A19A5F4C8217B2BD276BF577F8AB67E20C8
SHA-256:	C16E4AA0467BB288E9B7A8E23AF9E084923127F13B777A94E995389FDAD54E5E
SHA-512:	E3A023A8FB4454C4C1A4C499A863FAF8A063CAC8AC163FEDAA5D292FA81D238BBE8F33015BEF8DCB4FE0E4E2E8AF595F82463AB1A670757237828AA698AED 1CA
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="1519388" />.. <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" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.254256478645708
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	62835e34e60c1.dll
File size:	442368
MD5:	5572213d17be7de71f36fa68eb6808a8
SHA1:	5e8b27d57f6c9dc02cf2e30d47f8ed439f0fa20e
SHA256:	f58f9c8e6a62223efa263da10850e188004471cb2be65264b7f91f27ebab0766
SHA512:	f015eb3c633c916227b19dc1e446d189ce8ebbb82cadf1c71d962e9d67d8d43defef437f0cb41974173e14c8fdc65808c74e4baacc723ecf0d4c87078566334d
SSDEEP:	6144:oE1iktxgcV9yjYJrTOkRLookGIw8OaDSOKdPmo6iJTk/DmpFkbakc+abuFGGGGGD:oE44xgcV9yjY1OkEGx/V72/DmSH6/
TLSH:	3894E00965216A6EC9DC273DC9E5D31B1DA2B75CD23E70BE3CF43C9F7AE5125820428A
File Content Preview:	MZ.....@.....(.....0...w+!.W....]v.....4.....Y^.....7.....x.....<.....A....., ...,%..... {.....7.o.....O.....4.....5.....@.....Rich...

File Icon

Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x4014d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3EC34607 [Thu May 15 07:47:19 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a2b7486f7219709bc441af397fbc35ab

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add ecx, FFFFFFFFh
call 00007F6A68D094CAh

Instruction
pop eax
pop eax
mov dword ptr [0041461Ch], eax
mov edx, dword ptr [00414738h]
sub edx, 00005289h
call edx
mov eax, ebx
mov dword ptr [00414618h], eax
mov eax, esi
mov dword ptr [00414610h], eax
mov dword ptr [00414620h], ebp
mov dword ptr [00414614h], edi
add dword ptr [00414620h], 00000004h
loop 00007F6A68D09477h
mov dword ptr [ebp+00h], eax
nop
nop
nop
push esp
push D72C767Ah
jbe 00007F6A68D0951Fh
xlatb
rcl dword ptr [edi+2E46AAC6h], cl
jle 00007F6A68D094F6h
in al, dx
mov eax, A897C0E8h
pushfd
xor al, D1h
push esi
shl dword ptr [edx+7D8B0393h], 4Fh
int3
pop ss
mov dh, 0Eh
push es
sub dword ptr [esi-0Ah], esp
xchg dword ptr [esp+edi*2], ebp
xor esi, dword ptr [esi]
mov eax, 7DE0500Fh
dec ebp
sar eax, FFFFFFDEh
mov byte ptr [379552ECh], al
std
test al, E7h
sub al, A4h
scasb
add ebx, dword ptr [edx]
pop es
xchg eax, ebx
dec edi
int B4h
cmpsd
int 35h
mov dh, BDh
mov byte ptr [ebp-1BA85C92h], dl
mov es, word ptr [esi+34867DB0h]
out dx, al
push ecx
mov ebx, 7D4347D0h
and al, B0h

Instruction
jbe 00007F6A68D09447h
sti
push ds
push cs
fpatan
clc
jl 00007F6A68D09510h
xor ebp, dword ptr [edi]
cmc
fstsw word ptr [esp+ebx*2-12A5E66Ah]
jp 00007F6A68D09497h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdd7c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6c000	0xf40	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0xb8	.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	0xb8a0	0xc000	False	0.0812784830729	data	1.12155002117	IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x121f	0x2000	False	0.187133789062	data	4.12151309824	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_MEM_READ
.data	0xf000	0x7ac0	0x6000	False	0.37646484375	data	6.00984449077	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_GPREL, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.crt	0x17000	0x1dcbd	0x1e000	False	0.988419596354	data	7.98105173778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x35000	0x2ca3b	0x2d000	False	0.988259548611	data	7.98162384749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x9f28	0xa000	False	0.602783203125	data	6.51663069246	IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0x1360	0x2000	False	0.223266601562	data	3.77920644751	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x62360	0x666	data	English	United States
RT_ICON	0x629c8	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x67228	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 331218944, next used block 4106092544	English	United States
RT_ICON	0x697d0	0xea8	data	English	United States
RT_ICON	0x6a678	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6af20	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6b488	0xb4	data	English	United States
RT_DIALOG	0x6b540	0x120	data	English	United States
RT_DIALOG	0x6b660	0x158	data	English	United States
RT_DIALOG	0x6b7b8	0x202	data	English	United States
RT_DIALOG	0x6b9c0	0xf8	data	English	United States
RT_DIALOG	0x6bab8	0xa0	data	English	United States
RT_DIALOG	0x6bb58	0xee	data	English	United States
RT_GROUP_ICON	0x6bc48	0x4c	data	English	United States
RT_VERSION	0x6bc98	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
USER32.dll	IsWindow, LockWorkStation, ExitWindowsEx, LoadCursorFromFileA, IsWindowEnabled, GetMessagePos, GetClassNameA, GetClientRect, GetUpdateRgn, GetWindowWord
KERNEL32.dll	GlobalFree, GetCommState, LockFile, EnumResourceTypesA, GetProcAddress, GetVolumePathNamesForVolumeNameW, GetShortPathNameW, GlobalMemoryStatus, WriteProcessMemory, GlobalFlags, GetFileTime, GetThreadLocale, LocalHandle, GetBinaryTypeA, GetModuleFileNameA
OLEAUT32.dll	LoadTypeLibEx
msvcrt.dll	strcoll, strftime, strtod, strncmp, fgetwc
GDI32.dll	GetCharWidthFloatA, GetTextMetricsW, GdiFlush, ExtEscape
ADVAPI32.dll	RegGetValueA, EnumServicesStatusExW, FreeEncryptionCertificateHashList, GetUserNameW, GetSidSubAuthorityCount

Version Infos

Description	Data
LegalCopyright	A Company. All rights reserved.

Description	Data
InternalName	
FileVersion	1.0.0.0
CompanyName	A Company
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	myfile.exe
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

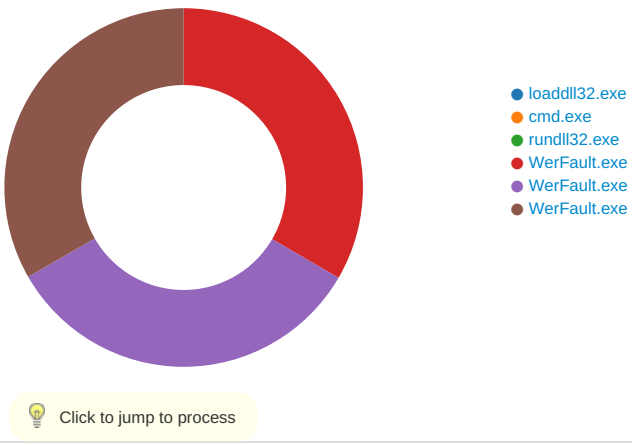
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.513.107.43.164 9772802033203 05/17/22-10:46:47.467879	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49772	80	192.168.2.5	13.107.43.16

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 10:58:37.038618088 CEST	49764	80	192.168.2.6	185.189.151.28
May 17, 2022 10:58:40.089255095 CEST	49764	80	192.168.2.6	185.189.151.28
May 17, 2022 10:58:46.105389118 CEST	49764	80	192.168.2.6	185.189.151.28
May 17, 2022 11:00:18.231358051 CEST	49808	80	192.168.2.6	185.189.151.70
May 17, 2022 11:00:21.342381001 CEST	49808	80	192.168.2.6	185.189.151.70
May 17, 2022 11:00:27.342931986 CEST	49808	80	192.168.2.6	185.189.151.70

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **7012**, Parent PID: **5148**

General

Target ID:	1
Start time:	10:57:57
Start date:	17/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll"
Imagebase:	0xb80000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7064**, Parent PID: **7012**

General

Target ID:	2
Start time:	10:57:57
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll",#1
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7120**, Parent PID: **7064**

General

Target ID:	3
Start time:	10:57:58
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe "C:\Users\user\Desktop\62835e34e60c1.dll",#1
Imagebase:	0x10c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.409022533.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.408311834.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.409143246.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.408868417.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.408399417.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.769433826.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.409166204.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.769302653.00000000049E9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.409046116.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.408598327.0000000004ED8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **1448**, Parent PID: **7012**

General

Target ID:	6
Start time:	10:58:02
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 400
Imagebase:	0xff0000
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	6DC51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp.xml	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC831.tmp.csv	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAE1.tmp.txt	success or wait	1	6DC4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 2c fd 62 fd 05 12 00 00 00 00 00	MDMP ,b	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	212	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 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 64 1b 00 00 25 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd%b0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	5722	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 14 6b 00 60 fd 56 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 20 00 00 00 4c fd 56 00 fd 14 6b 00 23 00 00 00 02 02 01 00 08 00 57 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++k`Vk LVk#W+	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	1632	168	68 1b 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd 56 00 00 00 00 00 fd 14 6b 00 00 00 00 00 01 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a 16 00 00	hVkZ	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	8586	20	0e 00 00 00 14 fd 56 00 00 00 00 00 fd 0c 00 00 6e 22 00 00	Vn"	success or wait	14	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	8814	3308	fd fd 2f 77 fd 1d 34 77 fd fd fd fd 48 fd 56 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 34 fd 56 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd fd 56 00 fd fd fd fd fd fd 56 00 12 12 34 77 fd 01 00 00 00 00 00 00 fd fd fd fd 68 fd 56 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3c fd 2f 77 00 00 00 00 fd fd fd fd 68 fd 56 00 18 fd 56 00 fd 01 00 00 00 00 7b 00 04 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd fd fd fd 68 fd 56 00 fd fd fd fd fd 56 00 fd 17 30 77 fd fd fd fd 00 00 00 00 fd fd 56 00 fd 0c 34 77 fd fd fd fd 00 00 00 00 18 fd 56 00 00 00 00 00 00 00 00 00 70 fd 56 00 0a 36 77 18 fd 56 00 68 fd 56 00 fd fd fd fd 68 fd 56	/w4wHV4VVV4whV</wh VV{hVV0wV4wV pV6wVhVhV	success or wait	13	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	27150	580	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 50 fd fd 00 1c fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd 00 fd 2d 00 00 fd 2d 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 70 fd fd 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 70 2d 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 54 72 2d 00 fd fd fd 00 60 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	/w-wP@-w@-w---0pp-Tr-`	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	6438	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 00 00 00 00 58 fd 56 00 fd fd 2f 77 23 00 00 00 06 02 00 00 18 fd 56 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++kXV/w#V+	success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 2e 00 00 00 00 00 fd fd fd 00 00 00 00 00 0c 03 00 00 5a 2f 00 00 fd 02 00 00 fd 1e 00 00	.Z/	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	4232	120	00 00 fd 73 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 1a 16 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	s`A!-aBB?#@A	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	5682	40	22 00 00 00 36 00 32 00 38 00 33 00 35 00 65 00 33 00 34 00 65 00 36 00 30 00 63 00 31 00 2e 00 64 00 6c 00 6c 00 00 00	"62835e34e60c1.dll	success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	4352	668	00 00 6b 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 32 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 02 00 00 00 00 00 fd 00 03 00 00 00 00 40 40 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 25 fd 03 00 00 00 00 00 25 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 09 1b 00 00 00 00 00 46 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 15 0b 05 00 00 00 00 00 66 fd 0d 7e 00 00 00 00 fd fd 67 1f 00 00 00 00 37 fd 7d 20 00 00 00 00 fd fd 16 01 00 00 00 00 fd 21 01 00 62 07 01 00 75 fd 05 00 0b fd 0a 00 46 fd 04 00 06 7f 15 00 15 0b 05 00 fd 01 2d 00 36 fd 01 00 fd 0f 13 00 00 00 00 00 1b 7e 1a 00 65 72 04	k5F>2Zb@@%%F@f~g7 } !buF-6~er	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	27730	6436	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB41C.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 fd 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 10 00 00 4e 75 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$!`8T(Nu	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7012</Pid>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1082	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 38 00 34 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8847</Uptime>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1230	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1320	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1380	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1434	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1530	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 35 00 32 00 30 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52019200</VirtualSize>	success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1616</PageFaultCount>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 30 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6000640</PeakWorkingSetSize>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1800	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 36 00 30 00 30 00 30 00 36 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>6000640</WorkingSetSize>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>100888</QuotaPeakPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2014	96	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 39 00 38 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98888</QuotaPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2120	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 31 00 35 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>15520</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2254	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 31 00 35 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>15168</QuotaNonPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>14 95040</Pe akPagefileUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848 </PrivateUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2640	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2694	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2734	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2828	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	2910	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 38 00 37 00 39 00 31 00 32 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5879128</Uptime>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3072	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3162	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3226	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	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3284	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3388	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3476	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 34 00 39 00 39 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>49905</PageFaultCount>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3566	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 30 00 33 00 37 00 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>103706624</PeakWorkingSetSize>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 31 00 38 00 31 00 31 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>98181120</WorkingSetSize>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3776	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 39 00 38 00 32 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>982544</QuotaPeakPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	3904	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 39 00 35 00 31 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>951880</QuotaPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4016	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 33 00 36 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>74360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4154	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 32 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>73272</QuotaNonPagedPoolUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4276	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 38 00 35 00 31 00 30 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>30851072</PagefileUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4368	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 33 00 36 00 37 00 32 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36720640</PeakPagefileUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4476	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 38 00 35 00 31 00 30 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>30851072</PrivateUsage>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4562	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4618	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4668	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4706	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4754	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4800	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	4860	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	9	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5548	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5594	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5632	4	0d 00 0a 00		success or wait	6	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5636	2	09 00		success or wait	12	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	5640	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6200	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6246	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6292	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6386	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6390	2	09 00		success or wait	2	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6394	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm, Inc.</SystemManufacturer>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6508	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm7,1</SystemProductName>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6604	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6608	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6612	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6732	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6736	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6740	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 30 00 32 00 31 00 32 00 34 00 35 00 34 00 37 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>1602124547</OSInstallDate>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6822	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6826	2	09 00		success or wait	2	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6830	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	6940	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7008	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7012	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7014	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7054	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7058	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7060	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7102	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7202	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7204	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	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7240	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7244	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7246	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7270	4	0d 00 0a 00		success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7274	2	09 00		success or wait	6	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7278	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 46 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000F</Flags>	success or wait	3	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7524	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7528	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7530	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7562	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T17:58:05Z">	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	2	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7670	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 34 00 30 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 31 00 32 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 36 00 34 00 33 00 37 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 36 00 34 00 33 00 37 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="403" PID="7012" UptimeMS="6437" TimeSinceCreationMS="6437" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7940	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7960	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7964	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	7966	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8010	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8056	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 36 00 38 00 66 00 66 00 39 00 31 00 66 00 2d 00 37 00 65 00 34 00 33 00 2d 00 34 00 38 00 31 00 37 00 2d 00 38 00 30 00 31 00 61 00 2d 00 34 00 32 00 30 00 37 00 64 00 37 00 30 00 36 00 31 00 30 00 66 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b68ff91f-7e43-4817-801a-4207d70610f3</Guid>	success or wait	1	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	2	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8162	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 30 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-17T17:58 :05Z</CreationTime>	success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8260	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8264	2	09 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8266	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8306	4	0d 00 0a 00		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBBE.tmp.WERInternalMetadata.xml	8310	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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4B8.tmp.xml	0	4665	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86\Report.wer	0	2	fd fd		success or wait	1	6DC4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86\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	146	6DC4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_cb7b105113bf417cfd7547dda3de839a49ae23_7cac0383_05f1cc86\Report.wer	8996	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 36 00 33 00 35 00 35 00 33 00 34 00 34 00 33 00	MetadataHash=-2063553443	success or wait	1	6DC4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{76a5be22-83c6-c2d9-c078-55b2e078b722}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DC636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DC61FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 56 00 EE 14 6B 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DC61FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 6480, Parent PID: 7012

General

Target ID:	9
Start time:	10:58:15
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 408
Imagebase:	0xff0000
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	722E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp.xml	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF434.tmp.csv	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81D.tmp.txt	success or wait	1	722D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 38 fd 62 fd 05 12 00 00 00 00 00	MDMP 8b	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	212	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 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 64 1b 00 00 25 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd%b0Pacific Standard TimePacific Daylight Time	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	5722	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 14 6b 00 60 fd 56 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 20 00 00 00 4c fd 56 00 fd 14 6b 00 23 00 00 00 02 02 01 00 08 00 57 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++k`Vk LVk#W+	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	1632	168	68 1b 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a 16 00 00	hZ	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	8586	20	0d 00 00 00 fd fd 56 00 00 00 00 00 34 0d 00 00 5e 22 00 00	V4^"	success or wait	13	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	8798	3380	fd fd 2f 77 fd 1d 34 77 fd fd fd fd 00 fd 56 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 34 fd 56 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd fd 56 00 fd fd fd fd fd fd 56 00 12 12 34 77 fd 01 00 00 00 00 00 00 fd fd fd fd 68 fd 56 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 56 00 07 1e 34 77 00 00 00 00 fd fd fd fd 68 fd 56 00 10 fd 56 00 fd 01 00 00 00 00 7b 00 04 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd fd fd fd 20 fd 56 00 fd fd fd fd fd fd 56 00 fd 17 30 77 fd fd fd fd 00 00 00 00 fd fd 56 00 fd 0c 34 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c fd 56 00 fd fd 32 77 10 fd 56 00 68 fd 56 00 00 00 00 00 68 fd 56	/w4wV4VVV4whVV4whVV{ VV0wV4wlV2wVhVhV	success or wait	12	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	26950	580	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 50 fd fd 00 1c fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd 00 fd 2d 00 00 fd 2d 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 70 fd fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 70 2d 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 54 72 2d 00 fd fd fd 00 60 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	/w-wP@-w@-w---0pp-Tr-`	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	1800	4	03 00 00 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	6438	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 00 00 00 00 10 fd 56 00 fd fd 2f 77 23 00 00 00 12 02 00 00 fd fd 56 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++kV/w#V+	success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 2e 00 00 00 00 00 fd fd fd 00 00 00 00 00 0c 03 00 00 fd 2f 00 00 fd 02 00 00 fd 1e 00 00	./	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	1960	4	16 00 00 00		success or wait	22	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	4232	120	00 00 fd 73 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 1a 16 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	s`A!-aBB?#@A	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	5682	40	22 00 00 00 36 00 32 00 38 00 33 00 35 00 65 00 33 00 34 00 65 00 36 00 30 00 63 00 31 00 2e 00 64 00 6c 00 6c 00 00 00	"62835e34e60c1.dll	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	4352	668	00 00 6b 00 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 32 16 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 60 fd 02 00 00 00 00 00 fd 00 03 00 00 00 00 6c 45 02 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 4d fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 43 1d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 49 05 00 00 00 00 00 32 fd fd 7f 00 00 00 00 2f 2f 41 20 00 00 00 00 fd fd fd 20 00 00 00 00 64 59 1e 01 00 00 00 00 fd 27 01 00 fd 1d 01 00 ff 05 00 7e fd 0a 00 43 1d 05 00 06 7f 15 00 fd 49 05 00 4e 01 3a 00 fd fd 01 00 fd 3c 16 00 00 00 00 00 57 14 25 00 1e 76 04	k5F>2Zb`lEMC@I2//AdY'~CIN:<W%v	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	27530	6436	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE28F.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 fd 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 10 00 00 fd 74 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$!`8T(t	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7012</Pid>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1082	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 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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 34 00 33 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20439</Uptime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1232	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1322	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1382	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1532	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 35 00 32 00 30 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52019200</VirtualSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 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>1651</PageFaultCount>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6021120</PeakWorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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 36 00 30 00 30 00 38 00 38 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6008832</WorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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 31 00 30 00 30 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>100888</QuotaPeakPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2016	96	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 39 00 38 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98664</QuotaPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17792</QuotaPeakNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17440</QuotaNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1495040</PeakPagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848</PrivateUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 38 00 39 00 30 00 37 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5890720</Uptime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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 35 00 31 00 36 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>51679</PageFaultCount>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.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 30 00 34 00 37 00 33 00 38 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>104738816</PeakWorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 39 00 34 00 32 00 39 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>98942976</WorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3778	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 39 00 38 00 32 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>982544</QuotaPeakPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	3906	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 39 00 33 00 35 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>935720</QuotaPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 33 00 36 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>74360</QuotaPeakNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 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>71912</QuotaNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 32 00 32 00 30 00 30 00 32 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>30220288</PagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 32 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36720640</PeakPagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 32 00 32 00 30 00 32 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>30220288</PrivateUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4802	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	4872	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	8	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5520	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5566	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5604	4	0d 00 0a 00		success or wait	6	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5608	2	09 00		success or wait	12	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	5612	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6166	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6172	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6218	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6264	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6358	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6362	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6366	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm, Inc.</SystemManufacturer>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6480	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm7,1</SystemProductName>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6576	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6580	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6584	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6712	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 30 00 32 00 31 00 32 00 34 00 35 00 34 00 37 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>1602124547</OSInstallDate>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6794	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6798	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6802	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6912	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	6986	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7032	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7074	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7176	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7218	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7250	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 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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7508	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7512	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7514	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7540	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7544	2	09 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7546	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 31 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T17:58:17Z">	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7646	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7650	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7654	266	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 34 00 30 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 31 00 32 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 31 00 33 00 35 00 36 00 32 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 31 00 33 00 35 00 36 00 32 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	<Process AsId="403" PID="7012" UptimeMS="13562" TimeSinceCreationMS="13562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7920	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7924	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7928	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7954	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	7998	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	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8036	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8040	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8044	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 36 00 38 00 30 00 36 00 66 00 37 00 61 00 2d 00 32 00 39 00 39 00 32 00 2d 00 34 00 37 00 39 00 62 00 2d 00 61 00 36 00 64 00 65 00 2d 00 65 00 36 00 31 00 38 00 37 00 30 00 37 00 38 00 66 00 37 00 39 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>86806f7a-2992-479b-a6de-e6187078f79f</Guid>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8142	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8146	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8150	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 31 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-17T17:58:17Z</CreationTime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8248	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8252	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8254	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8294	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE908.tmp.WERInternalMetadata.xml	8298	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	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREF72.tmp.xml	0	4598	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077\Report.wer	0	2	fd fd		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077\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	147	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b48bc1255c8639c941b68601e9389dc647932d2_7cac0383_190a0077\Report.wer	9074	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 35 00 31 00 31 00 33 00 37 00 32 00 32 00 34 00 35 00	MetadataHash=511372245	success or wait	1	722D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{99af11ac-21e7-0615-eb7e-1489e229fedd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	722F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 56 00 EE 14 6B 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	722F1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **3272**, Parent PID: **7012**

General

Target ID:	14
Start time:	10:58:25
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7012 -s 436
Imagebase:	0xff0000
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	722E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp.xml	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE6.tmp.csv	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D68.tmp.txt	success or wait	1	722D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 42 fd 62 fd 05 12 00 00 00 00 00	MDMP Bb	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	212	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 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 64 1b 00 00 25 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd%b0 Pacific Standard TimePacific Daylight Time	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	5722	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 14 6b 00 60 fd 56 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 20 00 00 00 4c fd 56 00 fd 14 6b 00 23 00 00 00 02 02 01 00 08 00 57 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++k`Vk LVk#W+	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	1632	168	68 1b 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 14 6b 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a 16 00 00	hkWZ	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	8586	20	10 00 00 00 00 fd 56 00 00 00 00 00 00 40 00 00 fd 22 00 00	V@"	success or wait	16	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	8846	16384	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	15	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	40014	580	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 50 fd fd 00 1c fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd 00 fd 2d 00 00 fd 2d 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 70 fd fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 70 2d 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 54 72 2d 00 fd fd fd 00 60 fd fd 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	/w-wP@-w@-w---0pp-Tr- `	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	1800	4	03 00 00 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	6438	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 14 6b 00 60 fd 56 00 00 00 00 00 fd 14 6b 00 fd fd fd fd 20 00 00 00 4c fd 56 00 fd 14 6b 00 23 00 00 00 02 02 01 00 08 00 57 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++k`Vk LVk#W+	success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 2e 00 00 00 00 00 fd fd fd 00 00 00 00 00 0c 03 00 00 fd 62 00 00 fd 02 00 00 fd 1e 00 00	.b	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	1960	4	16 00 00 00		success or wait	22	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	4232	120	00 00 fd 73 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 1a 16 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	s`A!-aBB?#@A	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	5682	40	22 00 00 00 36 00 32 00 38 00 33 00 35 00 65 00 33 00 34 00 65 00 36 00 30 00 63 00 31 00 2e 00 64 00 6c 00 6c 00 00 00	"62835e34e60c1.dll	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	4352	668	00 00 6b 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 32 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 00 03 00 00 00 00 fd 46 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3d fd 03 00 00 00 00 00 4d fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 22 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 49 05 00 00 00 00 00 fd 1e 42 00 00 00 00 6a 0d 32 21 00 00 00 00 fd fd 2f 21 00 00 00 00 16 76 28 01 00 00 00 00 fd 2c 01 00 7c 34 01 00 fd fd 05 00 39 fd 0a 00 fd 22 05 00 06 7f 15 00 fd 49 05 00 fd fd 45 00 fd fd 01 00 48 6d 19 00 00 00 00 00 fd 6d 2e 00 fd 78 04	k5F>2ZbF=M"@Ij2!/!v(,|49"IEHmm.x	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	40594	6376	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB73.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 04 01 00 00 fd 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 00 10 00 00 7a fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$l`8Tz	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7012</Pid>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1082	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 31 00 36 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>31650</Uptime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1232	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1322	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1382	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1532	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 35 00 32 00 30 00 31 00 35 00 31 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>52015104</VirtualSize>	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1695</PageFaultCount>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 34 00 35 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6045696</PeakWorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 36 00 30 00 34 00 35 00 36 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6045696</WorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 31 00 30 00 30 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>100888</QuotaPeakPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2016	96	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 39 00 38 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98656</QuotaPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>19168</QuotaPeakNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19032</QuotaNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1495040</PeakPagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848</PrivateUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 30 00 31 00 39 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5901931</Uptime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 35 00 33 00 33 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>53364</PageFaultCount>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 30 00 34 00 37 00 33 00 38 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>104738816</PeakWorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.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 30 00 34 00 32 00 35 00 35 00 34 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>104255488</WorkingSetSize>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3780	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 39 00 38 00 32 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>982544</QuotaPeakPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	3908	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 39 00 33 00 36 00 31 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>936152</QuotaPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4020	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 33 00 36 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>74360</QuotaPeakNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>72456</QuotaNonPagedPoolUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 35 00 36 00 31 00 34 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>35561472</PagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4372	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 32 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36720640</PeakPagefileUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 35 00 36 00 31 00 34 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>35561472</PrivateUsage>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4566	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4622	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4672	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4710	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4758	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4804	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	4874	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	8	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5488	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5534	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5572	4	0d 00 0a 00		success or wait	6	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5576	2	09 00		success or wait	12	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	5580	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6140	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6186	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6224	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6228	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6232	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6326	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6330	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6334	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm, Inc.</SystemManufacturer>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6440	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6444	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6448	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 73 00 69 00 6d 00 70 00 78 00 6d 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>simpxm7,1</SystemProductName>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6544	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6548	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6552	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6672	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6676	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6680	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 30 00 32 00 31 00 32 00 34 00 35 00 34 00 37 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>1602124547</OSInstallDate>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6762	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6766	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6770	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6872	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6876	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6880	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6954	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7000	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7042	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7144	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	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7186	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	6	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7218	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7470	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7502	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 32 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T17:58:28Z">	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7610	266	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 34 00 30 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 31 00 32 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 31 00 33 00 35 00 36 00 32 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 31 00 33 00 35 00 36 00 32 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	<Process AsId="403" PID="7012" UptimeMS="13562" TimeSinceCreationMS="13562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7876	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7880	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7884	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7910	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7954	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8000	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 37 00 33 00 33 00 39 00 66 00 33 00 35 00 2d 00 37 00 33 00 38 00 39 00 2d 00 34 00 62 00 66 00 32 00 2d 00 62 00 39 00 62 00 61 00 2d 00 32 00 37 00 63 00 30 00 61 00 63 00 34 00 64 00 37 00 30 00 36 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>67339f35-7389-4bf2-b9ba-27c0ac4d7069</Guid>	success or wait	1	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8098	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8102	2	09 00		success or wait	2	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8106	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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 32 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-17T17:58:28Z</CreationTime>	success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8208	2	09 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8210	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER150A.tmp.WERInternalMetadata.xml	8254	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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20C3.tmp.xml	0	4564	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 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	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db\Report.wer	0	2	fd fd		success or wait	1	722D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db\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	147	722D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_99e41d792528612ced890929ed2335749e1b7_7cac0383_0c9233db\Report.wer	9040	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 31 00 32 00 33 00 38 00 34 00 34 00 33 00 31 00	MetadataHash=1612384431	success or wait	1	722D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4abf9a9c-a5df-3978-2a81-cfb02abd7c7c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	722F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 EE 14 6B 00 02 00 00 00 01 00 00 00 04 00 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	722F1FE8	RegSetValueExW

Disassembly

No disassembly