

JoeSandbox Cloud BASIC



ID: 694555

Sample Name:

OCVOXxB3d1.dll

Cookbook: default.jbs

Time: 23:46:11

Date: 31/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report OCVOXxB3d1.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Initial Sample	4
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	6
Networking	6
Spam, unwanted Advertisements and Ransom Demands	6
System Summary	6
Data Obfuscation	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	10
General Information	10
Warnings	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	11
ASNs	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320\Report.wer	11
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\Report.wer	11
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\Report.wer	12
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	12
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	12
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	13
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	13
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	13
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp.xml	14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp.xml	14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp.xml	15
Static File Info	15
General	15
File Icon	15
Static PE Info	15
General	15
Entrypoint Preview	16
Rich Headers	17
Data Directories	17
Sections	17
Resources	18
Imports	18
Exports	18
Possible Origin	18
Network Behavior	18
Statistics	19
Behavior	19
System Behavior	19
Analysis Process: loaddll32.exePID: 5964, Parent PID: 2452	19
General	19
File Activities	19
Analysis Process: cmd.exePID: 1312, Parent PID: 5964	20
General	20
File Activities	20

Analysis Process: rundll32.exePID: 1308, Parent PID: 5964	20
General	20
File Activities	20
Analysis Process: rundll32.exePID: 1236, Parent PID: 1312	21
General	21
File Activities	21
Analysis Process: WerFault.exePID: 5860, Parent PID: 1236	21
General	21
File Activities	21
File Created	21
File Deleted	22
File Written	22
Registry Activities	44
Key Created	44
Key Value Created	44
Analysis Process: WerFault.exePID: 5832, Parent PID: 1308	44
General	44
File Activities	45
File Created	45
File Deleted	45
File Written	45
Registry Activities	67
Key Created	67
Key Value Created	67
Analysis Process: WerFault.exePID: 5976, Parent PID: 5964	68
General	68
File Activities	68
File Created	68
File Deleted	69
File Written	69
Registry Activities	91
Key Created	91
Disassembly	91

Windows Analysis Report

OCVOXxB3d1.dll

Overview

General Information

Sample Name:

OCVOXxB3d1.dll

Analysis ID:

694555

MD5:

6691e824d3f1dfe..

SHA1:

19af8b88be376c..

SHA256:

2f37a4c72c53bfb..

Tags:

dll

Infos:

Yara

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Gandcrab, ReflectiveLoader

Score: 96

Range: 0 - 100

Whitelisted: false

Confidence: 100%

Signatures

Antivirus / Scanner detection for sub...

Yara detected Gandcrab

Multi AV Scanner detection for subm...

Antivirus detection for URL or domain

Malicious sample detected (through...

Yara detected ReflectiveLoader

Found Tor onion address

Machine Learning detection for sam...

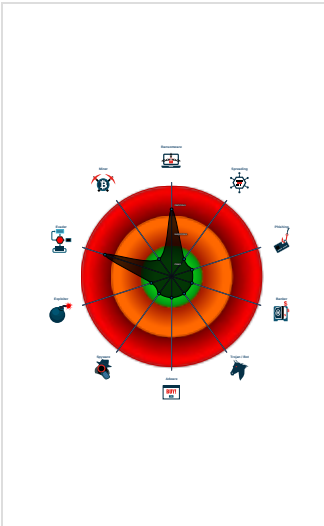
Uses 32bit PE files

Yara signature match

One or more processes crash

Uses code obfuscation techniques (...)

Classification



Process Tree

System is w10x64

loaddll32.exe (PID: 5964 cmdline: loaddll32.exe "C:\Users\user\Desktop\OCVOXxB3d1.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)

cmd.exe (PID: 1312 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\OCVOXxB3d1.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 1236 cmdline: rundll32.exe "C:\Users\user\Desktop\OCVOXxB3d1.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 5860 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1236 -s 632 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

rundll32.exe (PID: 1308 cmdline: rundll32.exe C:\Users\user\Desktop\OCVOXxB3d1.dll, ReflectiveLoader@0 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 5832 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1308 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

WerFault.exe (PID: 5976 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5964 -s 580 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
OCVOXxB3d1.dll	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	0x11832:\$x1: ReflectiveLoader

Copyright Joe Security LLC 2022

Page 4 of 91

Source	Rule	Description	Author	Strings
OCVOXxB3d1.dll	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	0x10ff6\$: DECRYPT.txt 0x11048\$: DECRYPT.txt
OCVOXxB3d1.dll	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
OCVOXxB3d1.dll	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
OCVOXxB3d1.dll	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	0x11831:\$s1: _ReflectiveLoader@ 0x11832:\$s2: ReflectiveLoader@
Click to see the 2 entries				

Memory Dumps				
Source	Rule	Description	Author	Strings
00000003.00000000.318645955.00000000707B3000.0000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.323778830.00000000707AB000.0000002.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.323778830.00000000707AB000.0000002.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000000.00000000.324075538.00000000707B3000.0000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.322931853.00000000707B3000.0000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 25 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
2.0.rundll32.exe.707a0000.1.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	0x10c32:\$x1: ReflectiveLoader
2.0.rundll32.exe.707a0000.1.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	0x103f6\$: DECRYPT.txt 0x10448\$: DECRYPT.txt
2.0.rundll32.exe.707a0000.1.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
2.0.rundll32.exe.707a0000.1.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
2.0.rundll32.exe.707a0000.1.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	0x10c31:\$s1: _ReflectiveLoader@ 0x10c32:\$s2: ReflectiveLoader@
Click to see the 37 entries				

Sigma Signatures	
No Sigma rule has matched	

Snort Signatures	
No Snort rule has matched	

Joe Sandbox Signatures	
------------------------	--

AV Detection



Antivirus / Scanner detection for submitted sample
Multi AV Scanner detection for submitted file
Antivirus detection for URL or domain
Machine Learning detection for sample

Networking



Found Tor onion address

Spam, unwanted Advertisements and Ransom Demands



Yara detected Gandcrab

System Summary



Malicious sample detected (through community Yara rule)

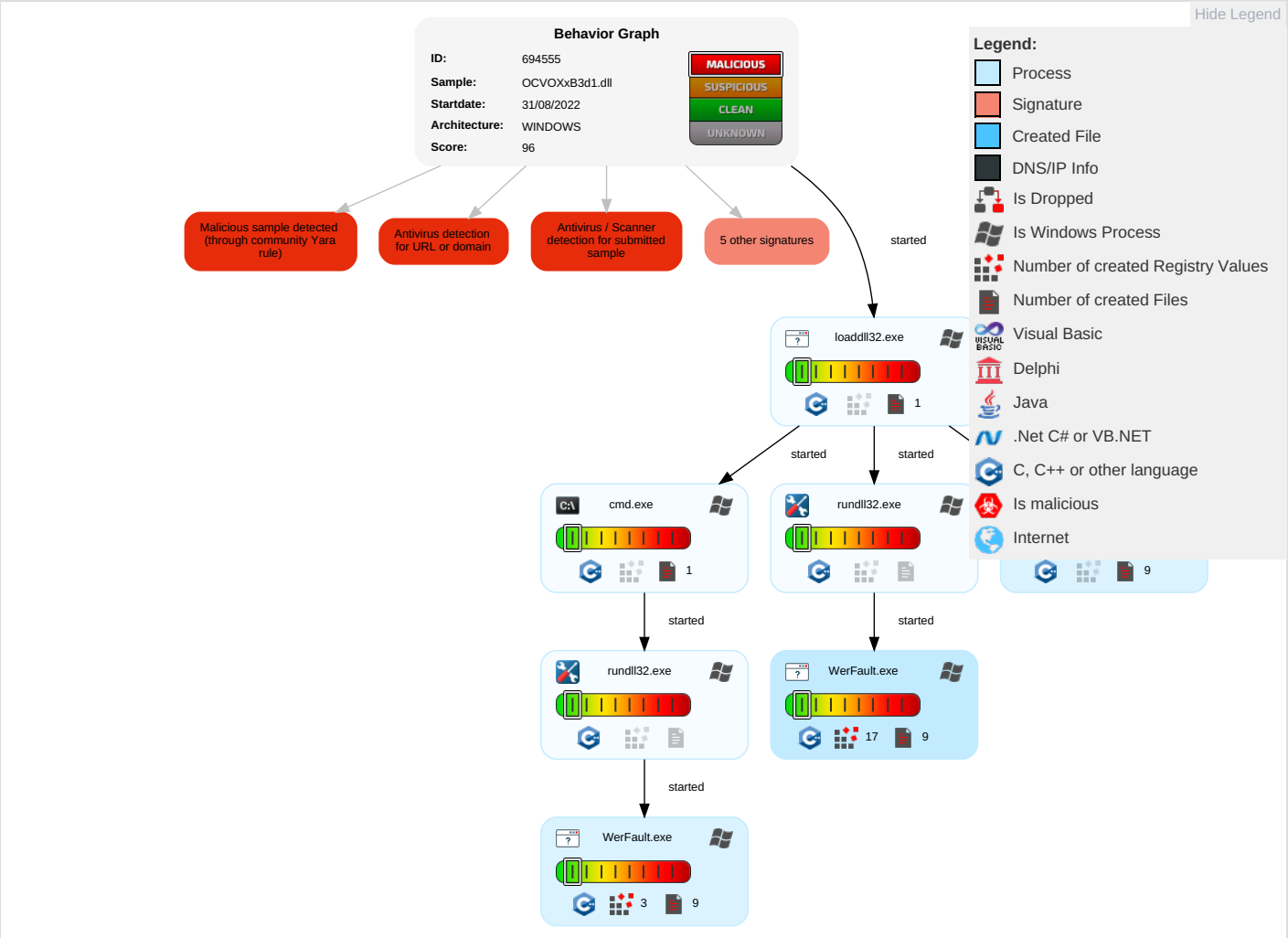
Data Obfuscation



Yara detected ReflectiveLoader

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	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Proxy	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Rundll32	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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 1 Process Injection	Security Account Manager	1 System Information 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OCVOXB3d1.dll	78%	Virustotal		Browse
OCVOXB3d1.dll	63%	Metadefender		Browse
OCVOXB3d1.dll	96%	ReversingLabs	Win32.Ransomwar e.GandCrab	
OCVOXB3d1.dll	100%	Avira	HEUR/AGEN.1239 798	
OCVOXB3d1.dll	100%	Joe Sandbox ML		

Dropped Files

 No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loadll32.exe.707a0000.0.unpack	100%	Avira	HEUR/AGEN.12 39798		Download File
3.0.rundll32.exe.707a0000.1.unpack	100%	Avira	HEUR/AGEN.12 39798		Download File
2.0.rundll32.exe.707a0000.1.unpack	100%	Avira	HEUR/AGEN.12 39798		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.rundll32.exe.707a0000.0.unpack	100%	Avira	HEUR/AGEN.1239798		Download File
3.0.rundll32.exe.707a0000.0.unpack	100%	Avira	HEUR/AGEN.1239798		Download File
0.0.loaddll32.exe.707a0000.1.unpack	100%	Avira	HEUR/AGEN.1239798		Download File

Domains

 No Antivirus matches

Source	Detection	Scanner	Label	Link
http://gandcrab2pie73et.onion/cb44cde56c4e43dc	100%	Avira URL Cloud	malware	
http://https://psi-im.org/download/	0%	Virustotal		Browse
http://https://psi-im.org/download/	0%	Avira URL Cloud	safe	
http://sj.ms/register.php	0%	Virustotal		Browse
http://sj.ms/register.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

 No contacted domains info

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sfu.ca/jabber/Psi_Jabber_PC.pdf	loadll32.exe, 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000000.318645955.0000000707B3000.00000008.00000001.01000000.00000003.sdmp, OCVOXxB3d1.dll	false		high
http://https://www.torproject.org/	loadll32.exe, 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000000.318645955.0000000707B3000.00000008.00000001.01000000.00000003.sdmp, OCVOXxB3d1.dll	false		high
http://gandcrab2pie73et.onion/cb44cde56c4e43dc	loadll32.exe, 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000000.318645955.0000000707B3000.00000008.00000001.01000000.00000003.sdmp, OCVOXxB3d1.dll	true	Avira URL Cloud: malware	unknown
http://https://psi-im.org/download/	loadll32.exe, 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000000.318645955.0000000707B3000.00000008.00000001.01000000.00000003.sdmp, OCVOXxB3d1.dll	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://sj.ms/register.php	loadll32.exe, 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, rundll32.exe, 00000003.00000000.318645955.0000000707B3000.00000008.00000001.01000000.00000003.sdmp, OCVOXxB3d1.dll	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694555
Start date and time:	2022-08-31 23:46:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OCVOXxB3d1.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.rans.evad.winDLL@10/12@0/0
EGA Information:	Failed
HDC Information:	Failed
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, eudb.ris.api.iris.microsoft.com, ctdl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target rundll32.exe, PID 1308 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

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_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320

\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):	0.8219435914224157
Encrypted:	false
SSDEEP:	96:6KJO4w+nYyTy9ha67QfHpXIQcQSc6mcEUcw3/s+a+z+HbHgXVG4rmMoVazWbSmfb:bwmnpHsieryjlq/u7sxlS274ItW
MD5:	95ACD9DF347422031C670B7066AC74BA
SHA1:	10525B285C7BDF86CD78FD174E3DE54C8D909162
SHA-256:	331A2996DA6529167C785EB044F4077E35028A54F9BB9FF1116D9B0FEA6CE343
SHA-512:	B294F88B7D4470BC27B513B075DD421D534FED10ED1CE0C37BA7338983E1853C5FCB51925C23501C5FFDF389D3DD1A057A620E4AD7CA73D0FC285281F694541
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.3.0.6.4.5.6.0.3.6.7.1.7.6.0.1.7.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....R.e.p.o.r.t.l.d.e.n.t.i.f.i.e.r.=6.d.c.0.1.3.1.8.-.e.7.8.f.-.4.1.c.c.-.a.3.5.b.-.d.e.1.3.c.3.c.f.3.b.1.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.l.d.e.n.t.i.f.i.e.r.=e.4.4.2.f.6.f.9.-.e.5.9.8.-.4.c.9.9.-.8.2.3.7.-.4.c.5.5.6.7.1.f.2.b.a.6.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=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.=0.0.0.0.1.7.4.c-.0.0.0.1-.0.0.1.f-.9.a.6.1-.2.1.3.8.8.3.b.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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!!0.0.0.0.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.l.d.=4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\

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):	0.9059728363114952
Encrypted:	false
SSDEEP:	192:Ni4F0oXvHKvgsv5yjed+s/u7sxlS274ItWc:Ni2XvKvgsv5yjeJ/u7sDX4ItWc
MD5:	0E43BD8D941E00246C3F93C725F58C00
SHA1:	103477A1BB721B5F45C1B9AAE92D3C5004DF8740
SHA-256:	C424147059729E531C6B3C3FCD54A7EF48787A3E8F14E763FFC1EA8D337B8E54
SHA-512:	25884F17DF579965EE2A8AD82454FD7009690130C6A633AA0EE9BAC6BEDE04740CF2E5F821A3B8E413B976F374C3106C33FE634D2282CFEBBBC422355C7EDF14
Malicious:	false

Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.3.0.6.4.5.6.0.3.5.2.2.8.8.7.4.5.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=0.f.f.6.9.3.6.c.-4.6.0.b.-4.3.a.9.-9.7.0.c.-4.9.e.9.d.b.a.8.7.e.6.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=c.a.3.4.5.8.0.6.-f.4.9.b.-4.d.7.4.-a.d.c.c.-d.b.e.f.1.f.e.d.d.0.9.2.....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.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.5.1.c.-0.0.0.1.-0.0.1.f.-c.2.0.8.-c.7.3.8.8.3.b.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.d.=W.:0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=1.9.8.6././0.1././3.0.:1.1.:4.2.:4.4.
----------	--

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\	
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):	0.9061603001604426
Encrypted:	false
SSDEEP:	192:eiDF0oXXHKvgsv5yjed+s/u7sxlS274ltWc:ei3X3Kvgsv5yjeJ/!u7sDX4ltWc
MD5:	783CD9979B465BD56A312A81AF23779A
SHA1:	29B7032B54142465F189F1AEE7748710FF5EBFB5
SHA-256:	3807EFA10516AB62401122798BBBD67B23AF952ABFEC4ABA8E583557C2237FEC
SHA-512:	1F4927BB2A1739DF6EFB1906AB6697F4C18840324AC832F580726BCE50530D052EF974131D081839588DC5CF79CD8572B03093525BF2BE0F1A2DE2628D50EB9E
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.3.0.6.4.5.6.0.3.5.2.2.2.1.5.4.3.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=b.a.3.3.4.1.c.d.-6.e.0.e.-4.d.f.4.-b.e.c.7.-3.3.f.c.e.4.b.8.6.7.5.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.=2.3.5.b.d.f.d.e.-4.2.c.5.-4.8.a.1.-b.0.8.f.-4.2.c.2.7.1.8.7.8.0.1.4.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.4.d.4.-0.0.0.1.-0.0.1.f.-7.7.7.b.-c.a.3.8.8.3.b.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.d.=W.:0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=1.9.8.6././0.1././3.0.:1.1.:4.2.:4.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Aug 31 21:47:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	43486
Entropy (8bit):	2.274269068482752
Encrypted:	false
SSDEEP:	192:pWpn6YVH3knleO5Skb9lt9duccFTKdM9TrRSi8M7XWMNCo8sbvn3:U3kl5Lbjtr3cbrRO4WMNCoT3
MD5:	1688DFDDC1A7CFFD64ABAE1D9FDF5B4B
SHA1:	B829431D220B16F3C17A2535A380A8B65624A314
SHA-256:	6B62B0BBDB73F05CACAE57352DB90055E6B0F94D72824FCAFD8B578545FB72F5
SHA-512:	D0B31EEED127279E27C4432988DBEA82E29E43C03D932F8D72C7403C6E7C329073B620062AA836934A88528C64AF94016C3532D3A614522C9BB64C6686F8551
Malicious:	false
Preview:	MDMP.....c.....\$.p.....T.....8.....T.....8.....U.....B.....GenuineIn telW.....T.....0.1.....E.u.r.o.p.e..S.t.a.n.d.a.r.d..T.i.m.e.....W...E.u.r.o.p.e..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\WER3F3A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Aug 31 21:47:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	44546
Entropy (8bit):	2.2181879012483754
Encrypted:	false
SSDEEP:	192:pxpn6YeHYD1+BrO5SkbTlhOPNWacqTfvRaNFFnTSs/FRmBpFLf!/fS:YU1+M5LbTKNqTfvAW4mTpX
MD5:	88AD55E140DCF676E1F10C35D308EEFA
SHA1:	79BC019333884EF72AC9BC04A8F692EC808C806A
SHA-256:	B98701697E90C5116F4588830C0A94BAE6C702982CF90A03F14E85715F035BFF
SHA-512:	3797FDF24B4AF08730EA694194D645D821C0AB367AB92A4A1204009F2D5912CAA5580C8644E3D16AB4C4543F16D8D05EBCC4FAE69DEE897483601C7739636B9
Malicious:	false

Preview:	MDMP.....c.....p-.....T.....8.....T.....U.....B.....GenuineIntelW.....T.....C.....0.1.....W... .Europe. .Standard. .Time.....W... .Europe. .Daylight. .Time.....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\WER4507.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Aug 31 21:47:17 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	49244
Entropy (8bit):	2.0375918571791765
Encrypted:	false
SSDEEP:	192:+8Vu5UeHny7OAOXzLtpRpCCcf/v/e+b3xFr8X+M/t8vKc:+hy7YXHtpRpc3Hew3Lr8X+0c
MD5:	E7CC47358ED5F64B03295BD8DB88DFCB
SHA1:	2BF9AEDCC11C1F2724D7BDAF396546B415C05736
SHA-256:	5BC1E47342D3F3553F48F8C96ADFF79E14B22903D4D73EA625676F263B854E22
SHA-512:	226FD21F0E7735205C2E4D702B8F10D01E0D22F148B00295088445333AC7717321E8D31AC5CA7D6ECC2CA845E80538FC55EA7B7D8499CBB5E19E2659428045E9
Malicious:	false
Preview:	MDMP.....c.....\.....\$.4.....T...*.....`.....8.....T.....D.....X.....D.....U.....B......GenuineIntelW.....T.....L.....C.....0.....W... .Europe. .Standard. .Time.....W... .Europe. .Daylight. .Time.....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\WER4575.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):	8252
Entropy (8bit):	3.6875080044315642
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLb6y6Ya496PgmfTUSJD+pBP89b9jmsfpfm:RrlsNiX6y6YF6PgmfTUSJ19jFfs
MD5:	6F9B680C0E9FD815034863A19A09F0CA
SHA1:	EF8AA76D4DFEBBA9FF3340A0D9579F435D130B91
SHA-256:	BA7DD8511B31E67468312420ABC7A5D438566594B9ADD94D5271171F6EC00A4
SHA-512:	268B672BD84BF35EF5BF28A84912D4BB240E7C4778734B90987AFCE87B1B390D33D69BD92391D9437BC6A89B659CED4098417948CAFB400A0E28DA8C51B1DD D
Malicious:	false
Preview:	..<?.xm.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.>(0x3.0):. .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.>1.2.3.6.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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):	8268
Entropy (8bit):	3.690507572614585
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivM6G6YBa867gmfTUSJD+pBo89b0PsfGcm:RrlsNiU6G6YBR67gmfTUSJg00fE
MD5:	5BAF0E9F6A37EB6F07C4CBBDD6EDED2F3
SHA1:	1F425F18A1ECF3DA4463BF7100F3FDEF47280CCA
SHA-256:	DAFE41118C94B84086C07FFD42C1FDB50B94CC231AE8E7BC1211192F1E939BD6
SHA-512:	C91B0452F18A6DC11C0C36A8F9A3D1A32E6A4C1183800C9855FF4A9B4F7A1DD938C5EF2506C60533120A0D944D8B05A29F751A7205D60C5BAB7AFE9E34A486F B
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.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>.1.3.0.8.</P.i.d>.....
----------	--

C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.4618065372208475
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWI9bqXIWgc8sqYj58fm8M4JCds4FH+q8/Ykn4SrS3d:ulTfklRgrsqYiJEGDW3d
MD5:	273FA6851D98B791A1CECC9313B2915A
SHA1:	E037D48FD99464850F5A9AD3FA478DE644EC3B9A
SHA-256:	BB7E6151582D13A2001C87D7F303C17CABFDB3C07066103E77530C6C13940DDB
SHA-512:	08EC2BC2AE2A53E1A8BF083AF2287EC4F12F583B0DA547B62CCA6C91816274B30E1C060D147116FA2BFE12F1DD8194EF9DA481F2FAA347E3DCDC0A22832CEE9
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="1672257" />..<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\WER4806.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.460891305904555
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWI9bqXIWgc8sqYjs8fm8M4JCds4FGd+q8/Yh4SrScd:ulTfklRgrsqYIJJd1DWcd
MD5:	28FCD77204FC00608F4BFF4357A62849
SHA1:	72FBF7B36FF9735BC7019AACC2C724A548DD8EEEE
SHA-256:	33A0DBABCEC16311ADF77B4013428E86D9D46C673D5E1BA78B9A36616B6C2EF1
SHA-512:	0AA5E01B0547DDD64E3F1B9CE9536745861D50B9CA24539059AEC495BFEDD80C63048E38FCF7C940BFC7880D9A6E6A0B1EE457CA0035FDF15412A6149CFA1F53
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="1672257" />..<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\WER495D.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):	8290
Entropy (8bit):	3.6909080311125346
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipil6V6YejSUCv4gmfdSwGN+pBY89b0Rsfqcm:RrlsNipp6V6YKSUo4gmfdSwX0KfK
MD5:	1A5328611B6731DD8F1FEDE0131B63FC
SHA1:	E8BD88E0C049147C34D40408BFA6BF7E285F4456
SHA-256:	DDC2E94C8077F58151A79623999842212BB140D0E10A54EF56CDC09E5C757CCD
SHA-512:	3EF014F3E35E451A23D764CE981507175A6D5E112E93DB14C94A53CD99DD59AA5B8F315401281702C538F64C67B6A486C0FABC9F726BF4D13B1E488FA82F37A
Malicious:	false

DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x5AF0C6DB [Mon May 7 21:36:27 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	1615a1cd5d3909399ee1f2121f6cefb

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 0Ch
mov dword ptr [ebp-0Ch], 00000001h
mov eax, dword ptr [ebp+0Ch]
mov dword ptr [ebp-08h], eax
cmp dword ptr [ebp-08h], 01h
je 00007F4044A91E16h
jmp 00007F4044A91E3Ch
jmp 00007F4044A91E3Ah
push 00000000h
push 00000000h
push 00000000h
push 002454E0h
push 00000000h
push 00000000h
call dword ptr [0024B1B8h]
mov dword ptr [ebp-04h], eax
cmp dword ptr [ebp-04h], 00000000h
je 00007F4044A91E1Ch
mov ecx, dword ptr [ebp-04h]
push ecx
call dword ptr [0024B0E0h]
mov eax, dword ptr [ebp-0Ch]
mov esp, ebp
pop ebp
retn 000Ch
int3
int3
push ebp
mov ebp, esp
sub esp, 5Ch
push esi
push 00000044h
lea eax, dword ptr [ebp-58h]
xorps xmm0, xmm0
push 00000000h
push eax
mov esi, ecx
movdqu dqword ptr [ebp-10h], xmm0
call 00007F4044A965A7h
mov eax, dword ptr [00253D18h]
add esp, 0Ch
mov dword ptr [ebp-18h], eax
mov dword ptr [ebp-1Ch], eax
mov eax, dword ptr [00253D14h]

Instruction
or dword ptr [ebp-2Ch], 00000101h
mov dword ptr [ebp-20h], eax
xor eax, eax
mov word ptr [ebp-28h], ax
lea eax, dword ptr [ebp-10h]
push eax
lea eax, dword ptr [ebp-58h]
mov dword ptr [ebp-58h], 00000044h
push eax
push 00000000h
push 00000000h
push 00000000h
push 00000001h
push 00000000h
push 00000000h
push esi
push 00000000h
call dword ptr [0024B0BCh]
test eax, eax
jne 00007F4044A91E1Dh
call dword ptr [0024B188h]
pop esi
mov esp, ebp
pop ebp
ret
push dword ptr [ebp-10h]

Rich Headers
Programming Language: • [C] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2013 build 21005 • [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x117f0	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11848	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16000	0xc30	.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	0xb000	0x27c	.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	0xa000	0xa000	False	0.433349609375	data	6.058990446424444	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0xb000	0x8000	0x8000	False	0.462799072265625	data	5.861163074824807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x1000	0x1000	False	0.2724609375	data	2.8951140973529945	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x14000	0x1000	0x1000	False	0.007568359375	ISO-8859 text, with no line terminators	0.00984533685142915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x1000	0x1000	False	0.06982421875	data	0.9533671901378512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x16000	0x1000	0x1000	False	0.658203125	data	5.847436562339401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x15060	0x17d	XML 1.0 document text	English	United States

Imports	
DLL	Import
KERNEL32.dll	Sleep, TerminateProcess, VerifyVersionInfoW, WaitForMultipleObjects, DeleteCriticalSection, LocalFree, ExpandEnvironmentStringsW, CreateProcessW, SetHandleInformation, IscratA, MultiByteToWideChar, CreatePipe, Process32FirstW, Process32NextW, CreateToolhelp32Snapshot, LeaveCriticalSection, CloseHandle, FindFirstFileW, GetFileAttributesW, IstrcmpW, MoveFileW, FindClose, FindNextFileW, SetFileAttributesW, GetNativeSystemInfo, GetComputerNameW, TerminateThread, GetWindowsDirectoryW, GetVolumeInformationW, LoadLibraryA, GetSystemDirectoryW, OpenProcess, InitializeCriticalSection, WaitForSingleObject, VerSetConditionMask, GetDriveTypeW, IstrcatW, IsProcessorFeaturePresent, IstrcmpiW, CreateFileMappingW, IstrlenW, ExitThread, CreateFileW, GetModuleFileNameW, WriteFile, GetModuleHandleW, UnmapViewOfFile, MapViewOfFile, GetFileSize, GetEnvironmentVariableW, IstrcpyA, GetModuleHandleA, VirtualAlloc, GetProcAddress, GetProcessHeap, HeapFree, CreateMutexW, IstrcpyW, GetLastError, SetFilePointerEx, LocalAlloc, GlobalFree, GetTempPathW, MulDiv, GlobalAlloc, GetTickCount, ReadFile, IstrcmpiA, VirtualFree, GetDiskFreeSpaceW, CreateThread, GetCurrentProcess, HeapAlloc, IstrlenA, EnterCriticalSection, ExitProcess
USER32.dll	DrawTextW, DrawTextA, GetDC, ReleaseDC, EndPaint, DestroyWindow, GetMessageW, LoadCursorW, BeginPaint, FillRect, TranslateMessage, RegisterClassExW, SetWindowLongW, MessageBoxA, wsprintfA, SystemParametersInfoW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, GetForegroundWindow, CharUpperBuffW, wsprintfW, LoadIconW
GDI32.dll	DeleteObject, SelectObject, CreateCompatibleDC, CreateCompatibleBitmap, SetPixel, GetObjectW, GetPixel, GetStockObject, TextOutW, SetBkColor, GetDIBits, GetDeviceCaps, DeleteDC, CreateFontW, SetTextColor
ADVAPI32.dll	RegCreateKeyExW, RegCloseKey, RegSetValueExW, OpenProcessToken, GetSidSubAuthority, GetSidSubAuthorityCount, GetTokenInformation, CryptExportKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, RegQueryValueExW, RegOpenKeyExW, AllocateAndInitializeSid, FreeSid, GetUserNameW
SHELL32.dll	SHGetSpecialFolderPathW, ShellExecuteW, ShellExecuteExW
CRYPT32.dll	CryptBinaryToStringA, CryptStringToBinaryA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

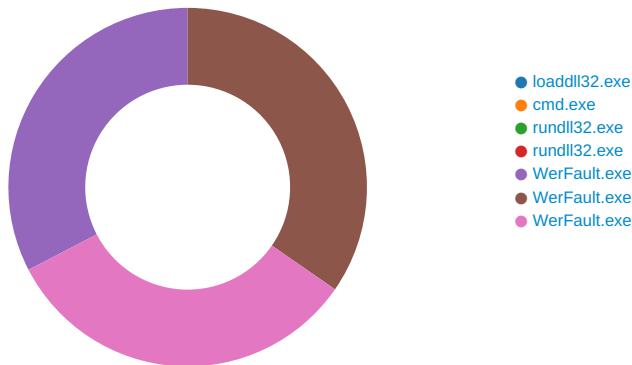
Exports		
Name	Ordinal	Address
_ReflectiveLoader@0	1	0x10006b40

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

Network Behavior

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5964, Parent PID: 2452

General

Target ID:	0
Start time:	23:47:08
Start date:	31/08/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\OCVOXxB3d1.dll"
Imagebase:	0xa60000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.323778830.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.323778830.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.324075538.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.322931853.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.336006148.000000000146B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.322923827.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.322923827.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.323325832.000000000146B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.322856833.000000000146B000.00000004.00000020.00020000.00000000.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
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 1312, Parent PID: 5964

General

Target ID:	1
Start time:	23:47:09
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\OCVOXxB3d1.dll",#1
Imagebase:	0xd90000
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: 1308, Parent PID: 5964

General

Target ID:	2
Start time:	23:47:09
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\OCVOXxB3d1.dll,_ReflectiveLoader@0
Imagebase:	0xaf0000
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_Gandcrab, Description: Yara detected Gandcrab, Source: 00000002.00000000.319338350.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000002.339378764.000000003590000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000000.319302985.000000003590000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000000.318756215.000000003590000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000002.00000000.319333495.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000000.319333495.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000002.00000000.318854091.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000002.00000000.318848277.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000000.318848277.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 1236, Parent PID: 1312

General

Target ID:	3
Start time:	23:47:09
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\OCVOxxB3d1.dll",#1
Imagebase:	0xaf0000
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_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000000.318645955.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000000.319112722.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000000.319112722.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000000.319117330.00000000707B3000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000000.318638611.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security - Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000000.318638611.00000000707AB000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: WerFault.exe PID: 5860, Parent PID: 1236

General

Target ID:	7
Start time:	23:47:13
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1236 -s 632
Imagebase:	0x1300000
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
-----------	--------	------------	---------	------------	-------	----------------	--------

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	6D771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp.xml	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48A0.tmp.csv	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C1D.tmp.txt	success or wait	1	6D76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 0f 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	7456	6	00 00 00 00 00 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	11924	1176	00 00 00 04 fd fd fd fd 00 00 fd 00 fd 7b fd 77 48 17 08 03 00 00 00 00 00 00 08 03 fd 79 fd 77 00 00 00 00 00 00 00 00 01 00 00 00 00 10 5c 77 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 00 00 fd 7b fd 77 fd fd fd fd 00 00 00 00 00 00 70 7f 00 00 00 00 30 07 70 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00	{wHyw\w{wp0p(Pm `fwPSwB	success or wait	17	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	32556	1772	fd fd fd 77 fd fd fd 77 58 02 00 00 fd fd fd 10 00 00 00 fd fd 1f 03 74 fd 1f 03 fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 fd fd 02 00 fd fd 02 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd 00 fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 06 09 03 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 50 0a 0a 03 00 00 00 00 00 00 00 00 fd 07 09 03 00 30 fd 02 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 30 fd 36 03 54 32 fd 02 38 fd 36 03 30 06 09 03 00 00 00 00 fd fd fd fd fd fd fd 00	wwXt@w@wXXP006T28 60	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	34328	9158	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 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 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPackettoCompletionTpWorkerFactor) ylRTimer(WaitCompletionPacketlRTim	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F2B.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 00 13 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 70 2d 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 38 19 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	\$p-T8T8	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 32 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1236</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1080	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 31 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7019</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1228	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1318	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1378	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 38 00 31 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>124981248</PeakVirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 37 00 33 00 30 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>124973056</VirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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 32 00 33 00 38 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>2389</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7905280</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7905280</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.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 38 00 30 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>180456</QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 32 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>180288</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2124	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 32 00 33 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23584</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2258	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 32 00 33 00 32 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>23232</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 30 00 30 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>512000</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 38 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5128192</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 30 00 30 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5120000 </PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2644	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2698	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2738	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1312</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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>cmd.exe</ImageName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2904	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 34 00 34 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7443</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3060	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3276	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 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3376	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 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3460	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 31 00 31 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>1114</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3548	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 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3678208</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 36 00 35 00 39 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>3665920</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 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 50 00 61 00 67 00 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>40960 </QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3878	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 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	3988	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 37 00 38 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>3407872</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 35 00 39 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3559424</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 37 00 38 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>3407872</PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4524	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4580	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4630	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4668	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4716	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4762	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 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>rundll32.exe</Parameter0>	success or wait	8	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5448	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5494	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	5540	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6100	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6146	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6192	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6294	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 64 00 72 00 6d 00 6b 00 66 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>drmkfe, Inc.</SystemManufacturer>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6408	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 64 00 72 00 6d 00 6b 00 66 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>drmke7,1</SystemProductName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6512	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>VMW71.0 0V.1822721 4.B64.2106252220</BIOSVersion>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6640	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 35 00 39 00 39 00 34 00 34 00 39 00 34 00 31 00 31 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1599449 411</OSInstallDate>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6730	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- 06-27T14:4 9:21Z</OSInstallTime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6840	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6916	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6962	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7004	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7106	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7148	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7180	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7432	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7464	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-31T21:47:16Z">	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7572	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 32 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 31 00 35 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 30 00 31 00 35 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="297" PID="1236" UptimeMS="1015" TimeSinceCreationMS="1015" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7834	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7838	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7842	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7862	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7866	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7868	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7912	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	7958	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 61 00 33 00 33 00 34 00 31 00 63 00 64 00 2d 00 36 00 65 00 30 00 65 00 2d 00 34 00 64 00 66 00 34 00 2d 00 62 00 65 00 63 00 37 00 2d 00 33 00 33 00 66 00 63 00 65 00 34 00 62 00 38 00 36 00 37 00 35 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ba3341cd-6e0e-4df4-bec7-33fce4b8675f</Guid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8064	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-31T21:47:16Z</CreationTime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8168	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4575.tmp.WERInternalMetadata.xml	8212	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER473B.tmp.xml	0	4630	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 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 3c 6f 73 3e 0d 0a 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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\Report.wer	0	2	fd fd		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\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	169	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16bd4e9c\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 34 00 38 00 36 00 30 00 37 00 34 00 38 00 30 00	MetadataHash=-648607480	success or wait	1	6D76497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D781FB2	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	05 00 00 C0 00 00 00 00 00 00 00 4C 58 7A 70 02 00 00 00 00 00 00 B8 B1 9E 60 00	success or wait	1	6D781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5832, Parent PID: 1308

General

Target ID:	8
Start time:	23:47:13
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1308 -s 648
Imagebase:	0x7ff61e220000
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	6D771717	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	

File Deleted					
File Path	Completion	Count	Source Address	Symbol	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp.xml	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A57.tmp.csv	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CE9.tmp.txt	success or wait	1	6D76497A	unknown	

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 0f 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	7456	6	00 00 00 00 00 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	6704	752	00 00 15 70 00 00 00 00 00 60 2e 00 fd 08 2e 00 fd fd 44 24 22 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd 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 fd 02 00 00 00 00 fd 50 01 00 00 01 00 00 00 00 00 00 fd fd fd 00 00 00 00 7d 7f 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 30 1b 00 00 00 00 00 63 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	p`..\$"BB?\${@AZbP}0c@	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	35496	9050	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIoIRTimer(WaitCompl	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F3A.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 00 13 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 70 2d 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 18 00 00 1a fd 00 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	p-T8T	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1308</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1080	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 32 00 33 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7236</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1228	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1318	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1378	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 38 00 31 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>12498 1248</PeakVirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 37 00 33 00 30 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>124973056 </VirtualSize>	success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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 32 00 33 00 39 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>2396</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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 37 00 39 00 32 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7925760</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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 37 00 39 00 32 00 35 00 37 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7925760</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.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 38 00 30 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>180456</QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 32 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>180288</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2124	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 32 00 33 00 37 00 31 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>23712</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2258	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 32 00 33 00 33 00 36 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>23360</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 35 00 32 00 37 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5152768</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5160960</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 35 00 32 00 37 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5152768</PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2644	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2698	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2738	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5964</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2832	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	2916	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 33 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8321</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3072	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3166	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3230	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3288	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 36 00 31 00 30 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>86106112</PeakVirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3388	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 34 00 39 00 33 00 30 00 35 00 36 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>84930560</VirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3472	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 38 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1892</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3560	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 39 00 35 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6955008</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3670	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 39 00 35 00 35 00 30 00 30 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>6955008</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3750	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3754	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3764	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 30 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>160440</QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3892	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 30 00 32 00 37 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>160272</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3990	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	3994	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4004	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 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>19800</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4128	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4132	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4142	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 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19448</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4250	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4254	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4264	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 35 00 32 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1527808</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4340	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4344	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4354	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 35 00 33 00 36 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1536000</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4446	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4450	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4460	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 35 00 32 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1527808</PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4532	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4536	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4544	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4590	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4594	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4600	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4642	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4646	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4650	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4682	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4686	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4688	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4730	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4734	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4736	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4774	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4778	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4782	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4844	4	0d 00 0a 00		success or wait	8	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4848	2	09 00		success or wait	16	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	4852	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 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>rundll32.exe</Parameter0>	success or wait	8	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5462	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5466	2	09 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5468	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5508	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5512	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5514	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5552	4	0d 00 0a 00		success or wait	6	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5556	2	09 00		success or wait	12	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	5560	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 .2.0.0.2 56.48</Parameter1>	success or wait	6	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6114	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6118	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6120	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6160	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6164	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6166	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6204	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6208	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6212	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-E 34B8D6354E8</MID>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6306	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6310	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6314	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 64 00 72 00 6d 00 6b 00 66 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>dr mkfe, Inc. </SystemManufacturer>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6420	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6424	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6428	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 64 00 72 00 6d 00 6b 00 66 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>d rmkfe7,1< SystemProductName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6524	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6528	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6532	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>VMW71.0 0V.1822721 4.B64.2106252220</BIO SVersion>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6652	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6656	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6660	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 35 00 39 00 39 00 34 00 34 00 39 00 34 00 31 00 31 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1599449 411</OSInstallDate>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6750	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6852	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6856	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6860	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6930	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6934	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6936	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6976	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6980	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	6982	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7024	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7126	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7168	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	6	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7200	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7446	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7450	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7452	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7478	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7482	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7484	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 00 3a 00 31 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-31T21:47:17Z">	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7584	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7588	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7592	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 33 00 30 00 38 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 35 00 34 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="296" PID="1308" UptimeMS="546" TimeSinceCreationMS="546" SuspendedMS="0" HangingCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7858	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7878	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7882	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7884	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7928	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	7974	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 66 00 66 00 36 00 39 00 33 00 36 00 63 00 2d 00 34 00 36 00 30 00 62 00 2d 00 34 00 33 00 61 00 39 00 2d 00 39 00 37 00 30 00 63 00 2d 00 34 00 39 00 65 00 39 00 64 00 62 00 61 00 38 00 37 00 65 00 36 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>0ff6936c-460b-43a9-970c-49e9dba87e62</Guid>	success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8072	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8076	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8080	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 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>2022-08-31T21:47:17Z</CreationTime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8184	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4640.tmp.WERInternalMetadata.xml	8228	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4806.tmp.xml	0	4630	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"?><reqver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\Report.wer	0	2	fd fd		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\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	169	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_bc4dba44e5104f2aa4617139c4a8f4569b60d283_82810a17_16914f67\Report.wer	11332	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 32 00 37 00 39 00 31 00 34 00 39 00 38 00 36 00 30 00	MetadataHash=279149860	success or wait	1	6D76497A	unknown

Registry Activities								
Key Created								
Key Path					Completion	Count	Source Address	Symbol
\REGISTRYVA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\PermissionsCheckTestKey					success or wait	1	6D7836BF	unknown
\REGISTRYVA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\PermissionsCheckTestKey					success or wait	1	6D7836BF	unknown
\REGISTRYVA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a					success or wait	1	6D7836BF	unknown
\REGISTRYVA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\PermissionsCheckTestKey					success or wait	1	6D7643D1	unknown

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	LowerCaseLong Path	unicode	c:\\windows\\syswow64\\rundll32.exe	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	LongPathHash	unicode	rundll32.exe ab97b57a	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D7836BF	unknown
\\REGISTRY\\A\\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\\Root\\InventoryApplicationFile\\rundll32.exe ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D7836BF	unknown
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D7836BF	unknown
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D7836BF	unknown
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	Language	dword	1033	success or wait	1	6D7836BF	unknown
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	IsPeFile	dword	1	success or wait	1	6D7836BF	unknown
\REGISTRYA\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	IsOsComponent	dword	1	success or wait	1	6D7836BF	unknown

Analysis Process: WerFault.exe PID: 5976, Parent PID: 5964	
General	
Target ID:	10
Start time:	23:47:15
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5964 -s 580
Imagebase:	0x1300000
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	6D771717	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D76497A	unknown

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp.xml				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB5.tmp.csv				success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5037.tmp.txt				success or wait	1	6D76497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	0	32	4d 44 4d 50 fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 0f 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	6364	6	00 00 00 00 00 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.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 18 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 4c 17 00 00 fd fd 0f 63 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UBGenuineIntel\WTLc0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	5576	120	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1c 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	v`A!-aBB?#@A	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	7378	34	1c 00 00 00 4f 00 43 00 56 00 4f 00 58 00 78 00 42 00 33 00 64 00 31 00 2e 00 64 00 6c 00 6c 00 00 00	OCVOXxB3d1.dll	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	5696	668	00 00 fd 73 00 00 00 00 00 70 01 00 00 00 00 00 fd fd fd 5a fd 1c 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 50 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 64 51 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 59 fd 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 3e 1b 00 00 00 00 00 43 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00 00 28 fd fd 6e 00 00 00 00 fd 2f fd 17 00 00 00 00 fd fd 72 10 00 00 00 00 fd 68 fd 01 00 00 00 00 fd fd 00 00 1a fd 00 00 fd fd 06 00 fd fd 0a 00 43 fd 04 00 06 fd 1f 00 fd fd 04 00 fd 4f 24 00 44 28 01 00 fd 75 0f 00 00 00 00 00 23 fd 14 00 fd 63 04	spZZbPdQY>C@(n/rhCO \$D(u#c	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	41112	8132	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	FileFileFileEvent(Wait CompletionPackettoCompletion TpWorkerFactory!RTimer(WaitCo mpletion	success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4507.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 5c 0e 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 34 16 00 00 05 00 00 00 54 01 00 00 fd 2a 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 18 16 00 00 44 fd 00 00 15 00 00 00 fd 01 00 00 58 16 00 00 16 00 00 00 fd 00 00 00 44 18 00 00	\\$4T*8TDXD	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5964</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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>loadl32.exe</ImageName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 31 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9123</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 36 00 31 00 30 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>86106112</PeakVirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 34 00 39 00 33 00 30 00 35 00 36 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>84930560</VirtualSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 39 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>1894</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 39 00 35 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6955008</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 39 00 35 00 35 00 30 00 30 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>6955008</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 36 00 30 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>160440</QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 30 00 32 00 37 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>160272</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>19800</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19448</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 35 00 32 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1527808</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 35 00 33 00 36 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1536000</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 35 00 32 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1527808</PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 35 00 31 00 31 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5851100</Uptime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 39 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>58960</PageFaultCount>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 30 00 31 00 31 00 31 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>120111104</PeakWorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 39 00 39 00 34 00 37 00 32 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>119947264</WorkingSetSize>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 39 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>1129624</QuotaPeakPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 39 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1089440</QuotaPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4024	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 31 00 35 00 33 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>81536</QuotaNonPagedPoolUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4284	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 34 00 39 00 37 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44449792</PagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4376	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 34 00 34 00 35 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>45445120</PeakPagefileUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4484	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 34 00 39 00 37 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4444979 2</PrivateUsage>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4570	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4626	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4676	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4714	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4762	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4808	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	4878	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5480	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5484	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5486	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5532	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	6	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	12	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	5578	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6132	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6136	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6138	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6184	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6230	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6324	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6328	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6332	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 64 00 72 00 6d 00 6b 00 66 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>drmkfe, Inc.</SystemManufacturer>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6446	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 64 00 72 00 6d 00 6b 00 66 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>drmkfe7,1</SystemProductName>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6542	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6546	2	09 00		success or wait	2	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6550	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>VMW71.0 0V.1822721 4.B64.2106252220</BIOSVersion>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6670	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6674	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6678	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 35 00 39 00 39 00 34 00 34 00 39 00 34 00 31 00 31 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1599449 411</OSInstallDate>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6768	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- 06-27T14:4 9:21Z</OSInstallTime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6870	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6874	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6878	70	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 2d 00 30 00 31 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>- 01:00</TimeZoneBias>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	6	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7218	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 00 3a 00 31 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-31T21:47:17Z">	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7610	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 35 00 37 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 35 00 37 00 38 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="294" PID="5964" UptimeMS="4578" TimeSinceCreationMS="4578" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7872	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7876	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7880	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7906	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7950	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	7996	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 64 00 63 00 30 00 31 00 33 00 31 00 38 00 2d 00 65 00 37 00 38 00 66 00 2d 00 34 00 31 00 63 00 63 00 2d 00 61 00 33 00 35 00 62 00 2d 00 64 00 65 00 31 00 33 00 63 00 33 00 63 00 66 00 33 00 62 00 31 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6dc01318-e78f-41cc-a35b-de13c3cf3b11</Guid>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8094	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8098	2	09 00		success or wait	2	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8102	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 37 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>2022-08-31T21:47:17Z</CreationTime>	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8204	2	09 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8206	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	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER495D.tmp.WERInternalMetadata.xml	8250	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	6D76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B81.tmp.xml	0	4558	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 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="verblid" val="	success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320\Report.wer	0	2	fd fd		success or wait	1	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320\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	157	6D76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_76b43c6d9c1a2a81832137409fd652e3d2404ae8_7cac0383_17015320\Report.wer	10138	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 33 00 30 00 34 00 38 00 33 00 36 00 33 00 33 00 33 00	MetadataHash=304836333	success or wait	1	6D76497A	unknown

Registry Activities				
Key Created				
Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1a1e7d09-340c-2d0e-c48a-917c89d42600}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D7836BF	unknown

Disassembly
 No disassembly