ID: 344139
Sample Name: BsYHxeX7Ok.dll
Cookbook: default.jbs
Time: 07:15:18
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

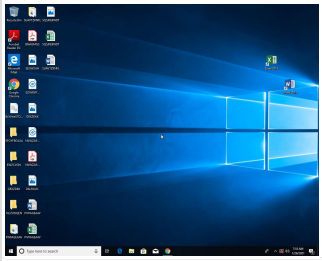
Analysis Report BsYHxeX7Ok.dll

Overview

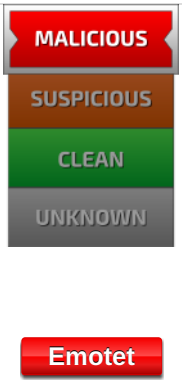
General Information

Sample Name:	BsYHxeX7Ok.dll
Analysis ID:	344139
MD5:	0125320a954399..
SHA1:	37afd871f306977..
SHA256:	d8a15d14d7bdc4..
Tags:	dll Heodo

Most interesting Screenshot:



Detection

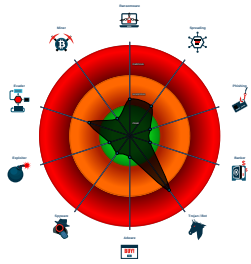


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains functionality to get notified…
- Contains functionality to read the PEB
- Contains functionality to shutdown / …
- Contains functionality to simulate m…
- Detected potential crypto function
- Monitors certain registry keys / valu…
- One or more processes crash
- PE file contains strange resources
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6404 cmdline: loaddll32.exe 'C:\Users\user\Desktop\BsYHxeX7Ok.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - WerFault.exe (PID: 6528 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 240 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6680 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 444 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 7016 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 472 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.282474266.0000000000850000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.282217417.0000000000710000.00000040.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.282441133.0000000000820000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Unpacked PEs

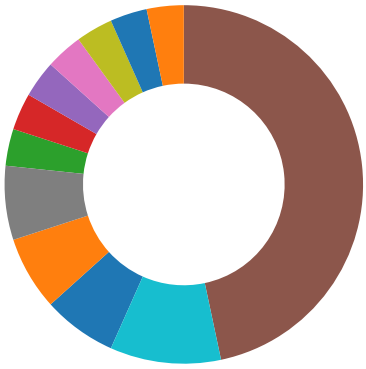
Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.710000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.loaddll32.exe.850000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.loaddll32.exe.850000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.710000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Binary contains paths to debug symbols

E-Banking Fraud:

Yara detected Emotet

Stealing of Sensitive Information:

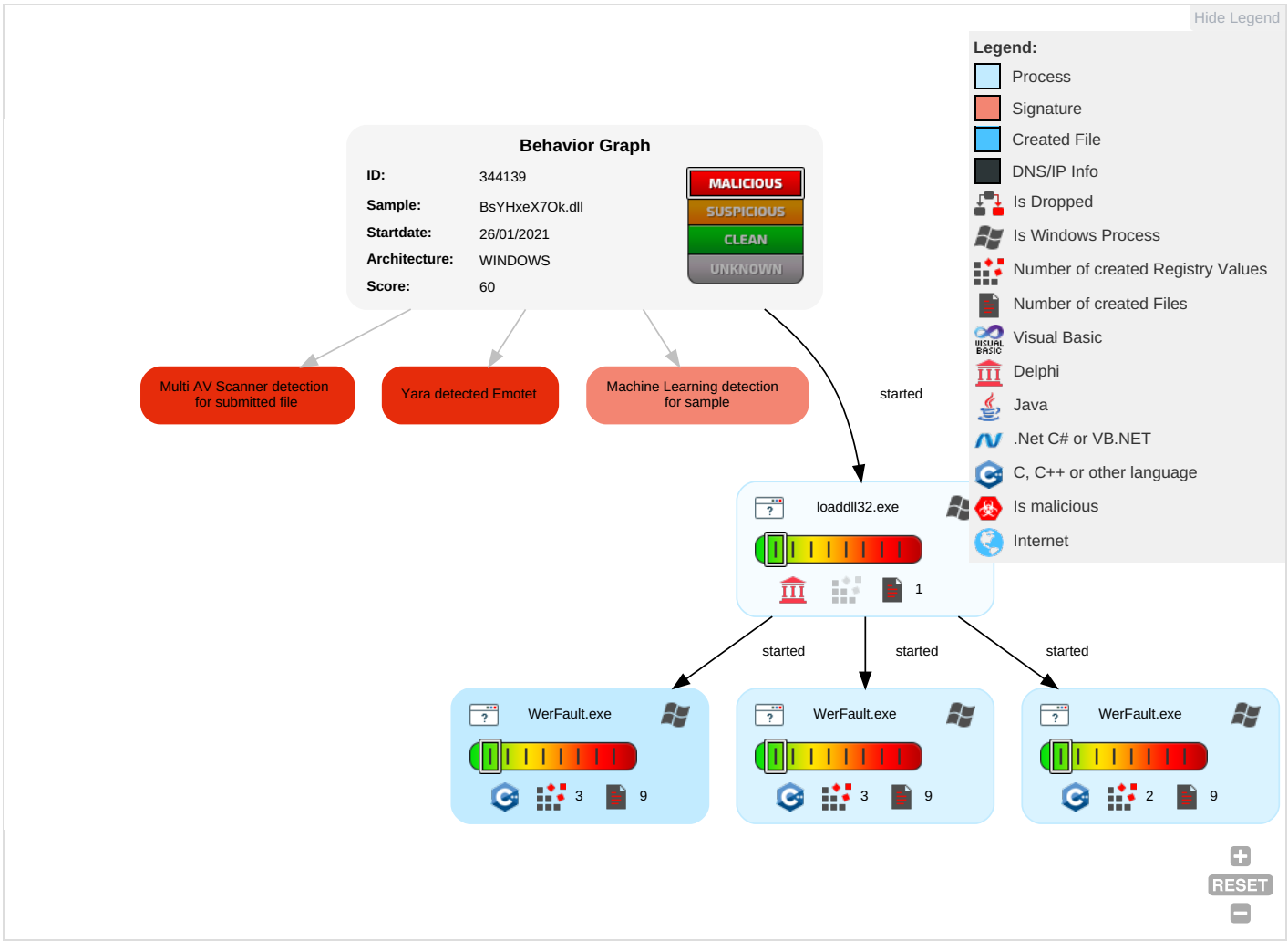
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Peripheral Device Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

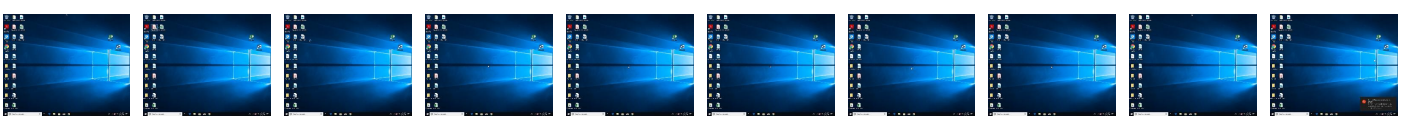
Behavior Graph

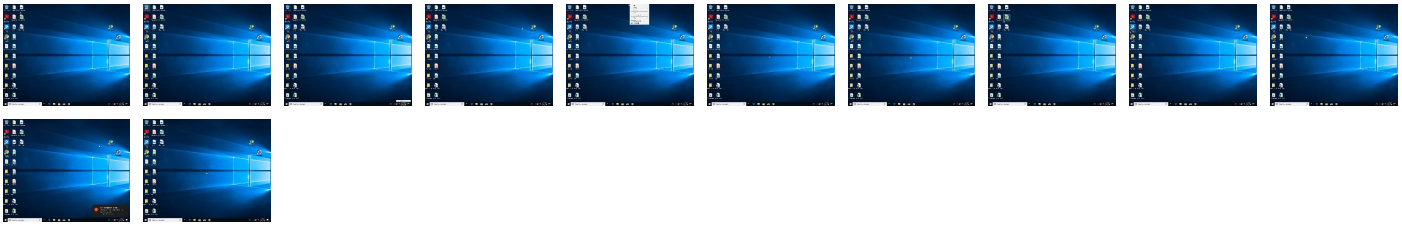


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BsYHxeX7Ok.dll	14%	Virustotal		Browse
BsYHxeX7Ok.dll	57%	ReversingLabs	Win32.Trojan.EmotetCrypt	
BsYHxeX7Ok.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.710000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoftmT9	0%	Avira URL Cloud	safe	
http://crl.microsoftmT	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://crl.microsoftmT9	WerFault.exe, 00000007.0000000 3.252976080.00000000047C7000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.microsoftmT	WerFault.exe, 00000007.0000000 3.252976080.00000000047C7000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344139
Start date:	26.01.2021
Start time:	07:15:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BsYHxeX7Ok.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
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:	mal60.troj.winDLL@4/12@0/0
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 93.9% • Quality standard deviation: 3.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.64.90.137, 104.43.193.48, 92.122.144.200, 51.11.168.160, 95.101.22.224, 95.101.22.216, 51.103.5.186, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
07:16:20	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10134
Entropy (8bit):	3.7646610495056536
Encrypted:	false
SSDEEP:	96:RYnj4CW0yTVy9hTot7JnqpXIQcQac6pcEccw35+a+z+HbHgEVG4rmMKazWbSmvFp:qjXUsH0tGtjpDH/u7s+S274ItWu
MD5:	C422BA0A5A2F8E68DE85C4F2B27F9744
SHA1:	3BF55DF103B0A07C910E7212E996086058E92EE2
SHA-256:	76F9281E1BBF7371B963688062377A17A0FF6C0EA433DA31BAF23F7607B0FD15
SHA-512:	A2CF62D79BE241ED893FC1D22D92A5584BB816D248509E744D6B853D6BC3F610290BEB393E370DA1008D9B711A11E2192F932F6A64E8AD36C30FA1C5AD2678F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.1.4.7.7.7.4.7.2.5.7.1.1.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.1.4.7.7.7.7.9.7.5.7.1.1.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.9.d.6.e.a.f.-.7.1.e.6.-.4.a.2.9.-.8.e.a.8.-.2.0.2.1.e.c.2.5.3.e.2.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.c.7.c.d.e.3.2.-.2.3.0.5.-.4.d.7.d.-.8.7.3.3.-.4.f.e.3.3.0.1.4.0.1.3.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.9.0.4.-.0.0.0.1.-.0.0.1.6.-.f.6.d.a.-.b.d.2.a.f.6.f.3.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10088
Entropy (8bit):	3.7615576725876148
Encrypted:	false
SSDEEP:	96:ox36Plcpj4CW0yEmqy9hT97efvpXIQcQPc6bcEycw37+a+z+HbHgEVG4rmMKazWG:E36SdXU/oHhfoXjpDH/u7sZS274ItWo
MD5:	7C12BFAB0F59B52846C04CA731DB267F
SHA1:	35D9E460CADC4404C6869BD59529D76B7D65F552
SHA-256:	1B1AAD60F962C1D569BFCE727AC594D027798D06BA38326D51FCFB41E7FCC265
SHA-512:	82B663750666DF8D20A7902E743E6304D570E6B48817CAD93D6E2A8750DC97081C2D1C21F59B2BAD1A5D546F56E60611207C4BAD7213C53875AB55179985120F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.1.4.7.7.8.6.0.0.6.9.5.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.1.4.7.7.9.0.2.5.6.9.4.4.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.9.1.d.f.a.c.c.-.1.3.c.a.-.4.d.e.1.-.b.4.1.7.-.5.e.b.2.d.c.5.f.0.1.5.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.d.6.2.6.9.f.0.-.5.5.2.e.-.4.3.7.3.-.a.7.1.f.-.7.5.e.6.d.e.a.3.0.0.6.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.0.4.-.0.0.0.1.-.0.0.1.6.-.f.6.d.a.-.b.d.2.a.f.6.f.3.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	9694
Entropy (8bit):	3.759141443436875
Encrypted:	false
SSDEEP:	96:ACj4CW0yxy9hT97WzSZpXIQcQac6pcEccw35+a+z+HbHgEVG4rmMKazWbSmvFVh/:XXU8H0tGtjpDy/u7s+S274ItbY
MD5:	C0C05C8B451A7A3E6C0931043ACAE82B
SHA1:	BBD9E48041A8C762CA2F04063102F83C6C58E2EC
SHA-256:	124FCECED0D204475F000701E1B296B48038426D5A1C0480FEEB189B8E19D338

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	
SHA-512:	5573A6CB152E6CCBE99D757B9019DD96FB534B8268E279C366226410F10477BC29BDF75F62A1040B5A824A1DF8FC2A1DB78D55E1BF0B6D81E669DBCA3CAF002
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.1.4.7.7.6.9.2.2.5.7.1.5.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.2.c.f.7.6.d.6.-.c.8.0.b.-.4.1.6.4.-.9.c.c.3.-.9.0.4.f.f.e.5.d.8.f.7.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.d.a.1.7.b.f.d.-.a.0.6.1.-.4.c.c.8.-.9.5.e.d.-.c.0.6.6.4.0.8.c.6.a.f.c.....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.=.0.0.0.0.1.9.0.4.-.0.0.0.1.-.0.0.1.6.-.f.6.d.a.-.b.d.2.a.f.6.f.3.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.3.0.:.1.2.:.1.5.:.2.1.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Jan 26 15:16:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	41828
Entropy (8bit):	2.038826544545495
Encrypted:	false
SSDEEP:	192:w0RghZKselJ94Q2S1uBIWrE91VNybNDXnpon/J/j:tRWZ5elJGQ2ScSWwPybN8Fj
MD5:	13F7C11E69DA9921F0651BDEF07D381B
SHA1:	E0892C6958FECCD7EEAF5387B7B8A4B841454185
SHA-256:	7A7A6DB3E948ADCFAEA494D9CEB767647D5BF746395B61BEBAC7B129117D7552
SHA-512:	297C0760F2705149595CB09F3170DB9DA313C8CBCE833C7C2C2C89519DC48427385BE4D7D6EFC4B69B4D15AD41FE11A0C01AB9260AC4175770E2243C40DA62
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....92.`.....U.....B.....GenuineIntelW.....T.....52.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.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):	8348
Entropy (8bit):	3.6920162098436102
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4DY6Qu2v6YIvSU8aigmfiSWCpN489bsn41fQkm:RrlsNiD6Z2v6YgSU8aigmfiS9snifi
MD5:	B087A84A63DCF6F547DED7B76CEA8618
SHA1:	0FE760CDC04A8A14D83F93FEC8BE0CB32B1A4415
SHA-256:	8EC704446CE8495B41A93C89D8C6ECFC9B8A969B6C01F3A19773B86A1D45CD63
SHA-512:	923B0462F9B50227320B7885D51437D4265C1F3A1A51256DCDF6BE16704DAA01EB039D193DFA5DA95E1606BD43D6AECCD2360DB4C88CB818B522D8BAB53E78E
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4658
Entropy (8bit):	4.429769617248258
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxRJgtWI9r2yWSC8B548fm8M4JONgFa2+q8vYNQxKcQIcQwv+ld:uITfxESSN/1JjKLxKkwv+ld
MD5:	15F23103DA45B2E2067424F685EEAC3B
SHA1:	0A0ECF39D509F43B7A4DDA03CC795ED7FDD98F35
SHA-256:	E7395CD429268F456A2870CFAA16863EEE1BE912FCFB1C984E05C37814307726
SHA-512:	0A25EAA7333E6DB9589FB4BA33CD61043AB5ECC0C0821F0681419D5561AFED3CCC99B61E04083688758C89137E26FE1A82D45EBF2A7BA78B3458EF2CAC9D38E

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp.xml	
Malicious:	false
Reputation:	low
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="833786" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Jan 26 15:16:15 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	41588
Entropy (8bit):	1.9841631652526566
Encrypted:	false
SSDEEP:	192:eTJghZKs+IJV4QLduBIWrNkSIyP0R57uClbfyS:IJWZ5+lJeQLESWR1IycmS
MD5:	765F4C728B13DB1896B73E947B12A075
SHA1:	3A442390A85D48F3C59F11EC23CD50616DF903EE
SHA-256:	90713247A4E4F0607D07381F754AE6FD3ABA76219BB96F45E4D8EEC59D43FF0F
SHA-512:	CC29B2948E90E7B937D9D3440C2D8C1E60365397E1AD1500116E4171F26485C11D364EE26B04B140A880073C7171910DA4C9C3F53F87A58C1B6EE64BB226F312
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....?2.`.....U.....B.....GenuineIntelW.....T.....52.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.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):	8324
Entropy (8bit):	3.6961754756167085
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4Dc67k2v6YI6SUqaRyegmf4SWCpr789bRnYsfzbm:RrlsNi36Y2v6Y1SUqawegmf4SiRnLfu
MD5:	62A4C5380C0701B801FB197677E5ABAC
SHA1:	4D292495B0B5F91FE005AE50849CAFABA41DBBA3
SHA-256:	75913919B52F091A4CE08D29F16A405613FC5E3D46BB781B98C4444AD14D4A5D
SHA-512:	3969A874806BBEE55F225514FA20B83BD0A33D7B78CBDBC6B5FF79DF564D3D1937EB3203607CCCEFB696C8AA6F4AF4715ACDD7FB32701BBEA2008A0E535D9F F7
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.0.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4597
Entropy (8bit):	4.472832368306633
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxRJgtWI9r2yWSC8BCa8fm8M4JO6ZFD+q8bDRxKcQIcQwv+kd:uITfxESSNkJ1XGRxKkwv+kd
MD5:	BC1B5B1EEC72DA00CD5949DC7F3BA676
SHA1:	E12EC1F3D79B613019F10A0045D0438CC00E1BCC
SHA-256:	1B18F4B5F4C9BFEBA22BADF0E6151A5E12F659825AD8D70BD4E646BB80C1E6F6
SHA-512:	CEE37113BD761A498F4F3E4EC6967A6254E339AE4FB5657EC08E286BD46DD4ECAAD9FE01C3B775B7C6AF0724369330DB21AD1EF0DB9FAC0828C24E80BD4028 71
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.xml	
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="833786" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Jan 26 15:16:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	38012
Entropy (8bit):	1.9487981955990552
Encrypted:	false
SSDEEP:	192:T9NhZKs+lJn4QjeuBlWrR79BK7EljefEgd:JNhZ5+lJ4QjlSWV9BLEy
MD5:	0B9AD215C68D0C2D8D4ECF2D37D404FA
SHA1:	E59D52ABA900ABB633313B1C1069C44EA413D5CD
SHA-256:	A2359A269A277B7C0C9F22E3B87C282F06660E5CD25522CC1B0261CE1010DF7F
SHA-512:	381A837F6896D77F9666D088D5126163C908D6289AF713FD96472AF7DFFDDDFB5AC17C971D5840CB9AEE8928ED6A3418D0AA6D6BB1581F94F1343ABA2CF90BE D
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....J2.`.....U.....B.....GenuineIntelW.....T.....52.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.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):	8284
Entropy (8bit):	3.6935941200272753
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4DK6ON2v6YIBSUqWJGgmfVSNCpDI89bgnYsfT6jAm:RrlsNiZ6U2v6YOSUqRgmfVSognLfex
MD5:	D3EF14C680659FAFE7857906EA45F07E
SHA1:	8E38362D0022974C6F9D4DE01928B9860149F470
SHA-256:	1CC0D42DE82F5B2CD5BF2DAEE353CC4C7D04908884ABAFB8B78401015163A0FA
SHA-512:	18C25D8A622E514729EBCB9BCAB71D67B40557689605E49746F35A412D04FE4B75C9E16C613D3BBCF4A502C444C142360DADEC758B703F01EB53FAF1E89683A
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.0.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4557
Entropy (8bit):	4.4437911607407345
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxKJgtWI9r2yWSC8Bk8fm8M4JORjFa5+q8p8nxKcQIcQwv+kd:uITf+ESSNnJ1bxKkwv+kd
MD5:	0299DEE8AB3686E56106BD95512135EE
SHA1:	99340B2A5043DCC5BC2953D621AA2A1193B649CF
SHA-256:	085A99D7E2E96BA20FDC7A439CD870BE4B5DBEBE288B8A411B9F9E2EDBC3D448
SHA-512:	913A7E69FF027B2E0FA6468B3AC9D02D316184596845B6B30B581F13B3E11F2D4BFD47D98E73795F3F13222B104D61C496788CA99B032B6E2AE44A06B48A75D4
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp.xml	
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="833787" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.906327751615201
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 97.97% • Win32 Executable Delphi generic (14689/80) 1.44% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	BsYHxeX7Ok.dll
File size:	628736
MD5:	0125320a954399ad7b275b67b97a273f
SHA1:	37afd871f306977f49c56400183ef5a80d8748f1
SHA256:	d8a15d14d7bdc4d2e1d948e20cf2835b452f46b2c0860ccd8147ee8d8a43adec
SHA512:	bc4b30147d97520ff627cf8e843ffe3619ae7423fe1da7f3e6b21a0452728c1ba944d5acb53c65ea07372db22f9fac5c850683a5e385335ad08f28c6d20e6951
SSDEEP:	12288:SYzchQVZnkmt/70MWugxPJZFpf0c1pHBbdJrs2xnd:d4KV5Hpt8bZHLXCA
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x463ebc
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7ed08afc6b0c9da85427ea1b02b1e145

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFC4h
mov eax, 00463C14h
call 00007FCAB4E9DD45h
mov dword ptr [0046666Ch], 00463928h
mov eax, 00000001h
call 00007FCAB4EFB23Dh
call 00007FCAB4E9B9FCh
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x67000	0x22ec	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x71000	0x2ba00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6a000	0x6ed4	.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	0x0	0x0	
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
CODE	0x1000	0x62ee8	0x63000	False	0.52030806108	data	6.5550941356	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x64000	0x14cc	0x1600	False	0.433948863636	data	4.11607326462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x66000	0xcd1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x67000	0x22ec	0x2400	False	0.359809027778	data	4.92726416893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x6a000	0x6ed4	0x7000	False	0.624232700893	data	6.67422538704	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x71000	0x2ba00	0x2ba00	False	0.685765132521	data	6.85431640563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
FF	0x71b2c	0x25c09	data	English	United States
RT_CURSOR	0x97738	0x134	data		
RT_CURSOR	0x9786c	0x134	data		
RT_CURSOR	0x979a0	0x134	data		
RT_CURSOR	0x97ad4	0x134	data		
RT_CURSOR	0x97c08	0x134	data		
RT_CURSOR	0x97d3c	0x134	data		
RT_CURSOR	0x97e70	0x134	data		
RT_BITMAP	0x97fa4	0x1d0	data		
RT_BITMAP	0x98174	0x1e4	data		
RT_BITMAP	0x98358	0x1d0	data		
RT_BITMAP	0x98528	0x1d0	data		
RT_BITMAP	0x986f8	0x1d0	data		
RT_BITMAP	0x988c8	0x1d0	data		
RT_BITMAP	0x98a98	0x1d0	data		
RT_BITMAP	0x98c68	0x1d0	data		
RT_BITMAP	0x98e38	0x1d0	data		
RT_BITMAP	0x99008	0x1d0	data		
RT_BITMAP	0x991d8	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0x992c0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 49, next used block 48059	Russian	Russia
RT_DIALOG	0x995a8	0x52	data		
RT_STRING	0x995fc	0x404	data		
RT_STRING	0x99a00	0x1cc	data		
RT_STRING	0x99bcc	0x188	data		
RT_STRING	0x99d54	0x1b0	data		
RT_STRING	0x99f04	0x218	data		
RT_STRING	0x9a11c	0xec	data		
RT_STRING	0x9a208	0x224	data		
RT_STRING	0x9a42c	0x33c	data		
RT_STRING	0x9a768	0x3d4	data		
RT_STRING	0x9ab3c	0x3a4	data		
RT_STRING	0x9aee0	0x3e8	data		
RT_STRING	0x9b2c8	0xf4	data		
RT_STRING	0x9b3bc	0xc4	data		
RT_STRING	0x9b480	0x2c0	data		
RT_STRING	0x9b740	0x478	data		
RT_STRING	0x9bbb8	0x3ac	data		
RT_STRING	0x9bf64	0x2d4	data		
RT_RCDATA	0x9c238	0x10	data		
RT_RCDATA	0x9c248	0x358	data		
RT_RCDATA	0x9c5a0	0x29c	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0x9c83c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c850	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c864	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c878	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c88c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c8a0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9c8b4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x9c8c8	0x14	data	Russian	Russia

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA

DLL	Import
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, TlsFree, TlsAlloc, LocalFree, LocalAlloc
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WinExec, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFileA, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CharUpperW, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerA, CharUpperBuffA, CharUpperA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoCreateInstance, CoUninitialize, CoInitialize
oleaut32.dll	CreateErrorInfo, GetErrorInfo, SetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
user32.dll	DdeCmpStringHandles, DdeFreeStringHandle, DdeQueryStringA, DdeCreateStringHandleA, DdeGetLastError, DdeFreeDataHandle, DdeUnaccessData, DdeAccessData, DdeCreateDataHandle, DdeClientTransaction, DdeNameService, DdePostAdvise, DdeSetUserHandle, DdeQueryConvInfo, DdeDisconnect, DdeConnect, DdeUninitialize, DdeInitializeA

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 07:16:01.119040012 CET	61733	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:01.178134918 CET	53	61733	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:01.209001064 CET	65447	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:01.256872892 CET	53	65447	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:02.487807035 CET	52441	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:02.546792030 CET	53	52441	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:03.683407068 CET	62176	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:03.739995003 CET	53	62176	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:05.011957884 CET	59596	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:05.059942961 CET	53	59596	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:05.960835934 CET	65296	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:06.011603117 CET	53	65296	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:07.402606964 CET	63183	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:07.450618029 CET	53	63183	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:08.767453909 CET	60151	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:08.826179981 CET	53	60151	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:10.116492033 CET	56969	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:10.164515972 CET	53	56969	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:13.290750980 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:13.341430902 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:18.910341024 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:18.958494902 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:27.058024883 CET	49992	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:27.119025946 CET	53	49992	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:31.141572952 CET	60075	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:31.192306995 CET	53	60075	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:34.584722042 CET	55016	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:34.632829905 CET	53	55016	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:42.898499012 CET	64345	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:42.954871893 CET	53	64345	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:50.643254042 CET	57128	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:50.691179037 CET	53	57128	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:56.036890030 CET	54791	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:56.092883110 CET	53	54791	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:56.728971958 CET	50463	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:56.788089037 CET	53	50463	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:57.551562071 CET	50394	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:57.608000994 CET	53	50394	8.8.8.8	192.168.2.5
Jan 26, 2021 07:16:58.070348024 CET	58530	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:16:58.121098995 CET	53	58530	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:00.018488884 CET	53813	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:00.077462912 CET	53	53813	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:00.651200056 CET	63732	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:00.707487106 CET	53	63732	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:01.280186892 CET	57344	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:01.330993891 CET	53	57344	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:01.361679077 CET	54450	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:01.425633907 CET	53	54450	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:02.171823025 CET	59261	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:02.230834007 CET	53	59261	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:02.438508034 CET	57151	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:02.494695902 CET	53	57151	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:05.021364927 CET	59413	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:05.077379942 CET	53	59413	8.8.8.8	192.168.2.5
Jan 26, 2021 07:17:05.499620914 CET	60516	53	192.168.2.5	8.8.8.8
Jan 26, 2021 07:17:05.555548906 CET	53	60516	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 6404 Parent PID: 5700

General

Start time:	07:16:05
Start date:	26/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\BsYHxeX7Ok.dll'
Imagebase:	0x1050000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.282474266.0000000000850000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.282217417.0000000000710000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.282441133.0000000000820000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 6528 Parent PID: 6404

General

Start time:	07:16:07
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 240
Imagebase:	0x240000
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	6DF61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp.xml	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DD8.tmp.csv	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FFB.tmp.txt	success or wait	1	6DF5497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 39 32 10 60 a4 05 12 00 00 00 00 00	MDMP........ ....92.`........	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 b8 15 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 04 19 00 00 35 32 10 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....52.`................. ....0................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6c ef 56 00 00 00 00 00 00 00 00 00 fb 75 00 00 1c 23 00 00 00 00 00 00 00 00 00 00 91 82 71 00 23 00 00 00 46 02 01 00 34 ef 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...l.V..........u...#...... ......q.#...F...4.V.+.........	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	168	08 19 00 00 00 00 00 00 09 04 00 c0 08 00 00 00 c4 e3 56 00 00 00 00 00 91 82 71 00 00 00 00 00 01 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 f0 18 00 00	.................V.......q...	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	20	10 00 00 00 00 90 39 00 00 00 00 00 98 04 00 00 24 25 00 00	......9.........$%..	success or wait	16	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 05 01 a0 7b ad 77 48 17 87 00 00 00 00 00 00 00 87 00 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 00 f8 7b ad 77 ff 07 01 00 00 00 00 00 00 00 11 7f 00 00 00 00 30 07 11 7f 00 00 21 7f 28 02 22 7f 50 06 23 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.............{.wH............y .w...............t..........A...... {.w................0.....!. (.".P.#.................m........ ....`f.w.. ....PS.w.........B......	success or wait	15	6DF5497A	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp</td><td>unknown</td><td>256</td><td>24 40 52 51 e8 72 f9 00 00 c7 44 24 38 b7 fc 00 00 8d 7c 24 3c 33 c0 83 c4 10 ab 33 f6 ab ab c7 44 24 10 26 99 00 00 c1 6c 24 10 09 c1 64 24 10 10 81 74 24 10 7c 47 41 df 81 74 24 10 12 34 0d df c7 44 24 14 ab 5b 00 00 c1 6c 24 14 06 c1 64 24 14 05 81 74 24 14 1b 6c 00 00 c7 44 24 40 e3 21 00 00 c1 64 24 40 03 81 44 24 40 b4 19 ff ff 81 4c 24 40 75 c0 62 af 81 74 24 40 fd e8 62 af 8b 45 3c 8b 7c 24 40 89 44 24 24 8b 5c 28 78 03 dd 8b 43 1c 8b 4b 20 03 c5 89 44 24 20 03 cd 8b 43 24 03 c5 89 4c 24 18 89 44 24 1c eb 24 8b 04 b9 8b 54 24 14 03 c5 8b 4c 24 10 50 e8 c9 34 00 00 35 04 34 01 5f 59 3b 44 24 3c 74 0c 8b 4c 24 18 47 3b 7b 18 72 d7 eb 2c 8b 44 24 1c 8b 74 24 20 0f b7 04 78 8b 34 86 03 f5 3b f3 72 17 8b 44 24 24 8b 44 28 7c 03 c3 3b f0 73 09 8b ce e8</td><td>$@RQ.r....D$8.....|$<3.....3
..
..D$.&....l$...d$...t$.|GA..t$
..4...D$..[...l$...d$...t$..l.
..D$@.!...d$@..D$@.....L$
@u.b.
.t$@..b..E<.|$@.D$$.\
(x...C..K ...D$
...C$...L$..D$..$....T$
....L$.P..4..5.4._Y;D$<t..L$
.G;{.r..,.D$..t$ ...x.4...;.r..D
$$.D(|..;.s....</td><td>success or wait</td><td>1</td><td>6DF5497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp</td><td>unknown</td><td>4</td><td>03 00 00 00</td><td>....</td><td>success or wait</td><td>3</td><td>6DF5497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp</td><td>unknown</td><td>716</td><td>3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 e2 56 00 bc 9a a2 77 23 00 00 00 16 02 00 00 c0 e1 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa</td><td>?............................
....
....
....
...................+...S...+.
..+...........................
..V....w#.........V.+.........
....
..............</td><td>success or wait</td><td>3</td><td>6DF5497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp</td><td>unknown</td><td>48</td><td>1c 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 3a 00 00 00 00 00 e0 f9 b6 00 00 00 00 00 20 06 00 00 00 78 00 00 cc 02 00 00 54 21 00 00</td><td>........ .... :.............
....x......T!..</td><td>success or wait</td><td>1</td><td>6DF5497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp</td><td>unknown</td><td>4</td><td>1b 00 00 00</td><td>....</td><td>success or wait</td><td>27</td><td>6DF5497A</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	27	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	120	00 00 d5 74 00 00 00 00 00 40 14 00 48 78 14 00 ad 9a 07 f5 b6 18 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 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 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	...t.....@..Hx..... .....B.....B?..... ....."..... ..@A.....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	34	1c 00 00 00 42 00 73 00 59 00 48 00 78 00 65 00 58 00 37 00 4f 00 6b 00 2e 00 64 00 6c 00 6c 00 00 00	....B.s.Y.H.x.e.X.7.O.k...d.l.l...	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	668	00 00 71 00 00 00 00 00 00 00 d0 09 00 00 00 00 00 19 5e 42 2a ce 18 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 40 8b 02 00 00 00 00 00 50 b2 02 00 00 00 00 9b 40 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 18 53 03 00 00 00 00 00 1d 53 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 5b 18 00 00 00 00 00 3d a4 07 00 00 00 00 00 40 ff 1f 00 00 00 00 00 87 b5 07 00 00 00 00 00 4a cb 81 4f 00 00 00 00 62 a1 bc 14 00 00 00 00 a8 25 5a 0c 00 00 00 00 e9 19 c6 00 00 00 00 00 24 8b 00 00 cf 8d 00 00 f6 02 04 00 20 04 08 00 3d a4 07 00 fb 7e 15 00 87 b5 07 00 c0 2f 1c 00 b4 1a 01 00 f0 0a 0d 00 00 00 00 00 e2 73 0e 00 19 36 04	..q.....^B*.....Zb ....@.....P .....@.....S.. .....S.....[.....=. .....@.....J..O.... b.....%Z.....$..... ...=....~...../.....s...6.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	6844	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	....F.i.l.e.....F.i.l.e..... ..F.i.l.e.....F.i.l.e..... E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9730.tmp.dmp	unknown	120	03 00 00 00 94 00 00 00 08 07 00 00 04 00 00 00 68 0b 00 00 a8 07 00 00 0e 00 00 00 24 00 00 00 10 13 00 00 05 00 00 00 04 01 00 00 20 24 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 90 11 00 00 1c 92 00 00 15 00 00 00 ec 01 00 00 34 13 00 00 16 00 00 00 98 00 00 00 20 15 00 00	.....h.....$. ..... $.....`... ....8.....T..... .....4..... ...	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.4.0.4.<./.P.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m. d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.3.6.5. <./.U.p.t.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 35 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.5.9.3.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.5.1.1.6.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 31 00 34 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.1.4.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 38 00 39 00 32 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.8.9.2.9.9.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 38 00 39 00 32 00 39 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.8.9.2.9.9.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.5.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.2.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 35 00 33 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.3.4.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 35 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.0.7.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 32 00 32 00 30 00 37 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.2.0.7.7.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.7.2.<./.P.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 35 00 36 00 35 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.7.5.6.5.4.5.<./.U.p.t.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 32 00 39 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.2.9.7.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 32 00 34 00 38 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.2.2.4.8.4.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 39 00 34 00 31 00 32 00 34 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.9.4.1.2.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 37 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.7.1.5.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 36 00 35 00 31 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.1.6.5.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.0.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 36 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.8.6.4.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 31 00 30 00 34 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.4.1.0.4.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 39 00 36 00 30 00 36 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.6.9.6.0.6.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 31 00 30 00 34 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.4.1.0.4.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.0.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.r.x.d.p.u.s.,. .I.n.c...</.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.r.x.d.p.u.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 35 00 32 00 31 00 35 00 37 00 39 00 34 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.1.5.7.9.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 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	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.F.<./.F.l.a.g.s.>.	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.1.0.Z.".>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 30 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 32 00 36 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 36 00 30 00 39 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.6.". .P.I.D.=.".6.4.0.4.". .U.p.t.i.m.e.M.S.=.".2.6.0.9. ". .T.i.m.e.S.i.n.c.e.C.r.e.a. t.i.o.n.M.S.=.".2.6.0.9.". .S. u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 32 00 63 00 66 00 37 00 36 00 64 00 36 00 2d 00 63 00 38 00 30 00 62 00 2d 00 34 00 31 00 36 00 34 00 2d 00 39 00 63 00 63 00 33 00 2d 00 39 00 30 00 34 00 66 00 66 00 65 00 35 00 64 00 38 00 66 00 37 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.2.c.f.7.6.d.6.-.c.8.0.b.-.4.1.6.4.-.9.c.c.3.-.9.0.4.f.f.e.5.d.8.f.7.0.<./.G.u.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.1.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDA.tmp.xml	unknown	4658	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	unknown	2	ff fe	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	151	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a074f448eb416fc5ae408d6a8da6168cd6117a23_b4806494_19c8a097\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 30 00 38 00 31 00 38 00 39 00 33 00 34 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.0.0.8.1.8.9.3.4.5.	success or wait	1	6DF5497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c3135ed7-ca7b-689f-752c-1fddbd364810}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DF71FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 C4 E3 56 00 91 82 71 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DF71FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 6680 Parent PID: 6404

General

Start time:	07:16:13
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 444
Imagebase:	0x240000
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	6DF61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	success or wait	1	6DF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	success or wait	1	6DF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.xml	success or wait	1	6DF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.csv	success or wait	1	6DF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB385.tmp.txt	success or wait	1	6DF54BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 3f 32 10 60 a4 05 12 00 00 00 00 00	MDMP........ ....?2.`........	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 b8 15 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 04 19 00 00 35 32 10 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....52.`................. ....0.................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6c ef 56 00 00 00 00 00 00 00 00 00 fb 75 00 00 1c 23 00 00 00 00 00 00 00 00 00 00 91 82 71 00 23 00 00 00 46 02 01 00 34 ef 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...l.V..........u...#...... ......q.#...F...4.V.+.........	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	168	08 19 00 00 00 00 00 00 a5 01 00 c0 01 00 00 00 00 00 00 00 00 00 00 00 4a 0c 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 f0 18 00 00	........................J.....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	20	0d 00 00 00 00 90 39 00 00 00 00 00 98 04 00 00 f4 24 00 00	......9..........$..	success or wait	13	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 05 01 a0 7b ad 77 48 17 87 00 00 00 00 00 00 00 87 00 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 00 f8 7b ad 77 ff 07 01 00 00 00 00 00 00 00 11 7f 00 00 00 00 30 07 11 7f 00 00 21 7f 28 02 22 7f 50 06 23 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.............{.wH............y .w...............t..........A...... {.w................0.....!. (.".P.#.................m........ ....`f.w.. ....PS.w.........B......	success or wait	12	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	1976	bc b1 a2 77 d6 c9 a0 77 c8 00 00 00 aa aa aa aa 10 00 00 dc f8 a6 00 a8 f9 a6 00 aa aa aa aa 40 c7 a0 77 40 c7 a0 77 aa aa aa aa 00 f0 39 00 00 f0 39 00 00 00 00 00 c8 00 00 00 aa aa aa aa c8 00 00 00 aa aa aa aa 00 f0 39 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa d8 7e 88 00 00 00 00 00 00 00 00 00 88 80 87 00 00 90 39 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa ac fa b6 00 54 92 39 00 b4 fa b6 00 f8 84 87 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w..................... ..@..w@..w......9...9......... ....9............... ....~.... ....9................. ....T. 9.............................	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 b8 e1 56 00 bc 9a a2 77 23 00 00 00 06 02 00 00 78 e1 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... ..V....w#.......x.V.+.........	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	48	1c 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 3a 00 00 00 00 00 e0 f9 b6 00 00 00 00 00 20 06 00 00 18 78 00 00 cc 02 00 00 54 21 00 00	.... :............. ....x......T!..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	4	1b 00 00 00	....	success or wait	27	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	27	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	120	00 00 d5 74 00 00 00 00 00 40 14 00 48 78 14 00 ad 9a 07 f5 b6 18 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 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 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	...t.....@..Hx..... .....B.....B?..... ....."..... ..@A.....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	34	1c 00 00 00 42 00 73 00 59 00 48 00 78 00 65 00 58 00 37 00 4f 00 6b 00 2e 00 64 00 6c 00 6c 00 00 00	....B.s.Y.H.x.e.X.7.O.k...d.l.l...	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	668	00 00 71 00 00 00 00 00 00 00 d0 09 00 00 00 00 00 19 5e 42 2a ce 18 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 90 20 02 00 00 00 00 00 50 b2 02 00 00 00 00 aa 44 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 76 ec 00 00 00 00 00 00 50 58 03 00 00 00 00 00 1b 65 02 00 00 00 00 00 d2 1f 0c 00 00 00 00 00 6e df 13 00 00 00 00 00 40 ff 1f 00 00 00 00 00 49 ed 13 00 00 00 00 00 dc c9 a0 4f 00 00 00 00 cb 6b 13 15 00 00 00 00 b3 5f b8 0c 00 00 00 00 68 d1 d9 00 00 00 00 00 5f 93 00 00 2e a5 00 00 d9 43 04 00 a3 cc 00 00 6e df 13 00 d1 af 17 00 49 ed 13 00 95 37 2a 00 ec 1e 01 00 3b e0 0d 00 00 00 00 00 77 c2 1b 00 d9 3e 04	..q.....^B*.....Zb ....P .....D.....v... ....PX.....e.....n. .....@.....I.....O.... .k....._.....h....._..... ...C.....n.....I....7*..... ;.....w....>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	6844	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	....F.i.l.e.....F.i.l.e..... ..F.i.l.e.....F.i.l.e..... E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACAC.tmp.dmp	unknown	120	03 00 00 00 94 00 00 00 08 07 00 00 04 00 00 00 68 0b 00 00 a8 07 00 00 0e 00 00 00 24 00 00 00 10 13 00 00 05 00 00 00 d4 00 00 00 20 24 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 90 11 00 00 2c 91 00 00 15 00 00 00 ec 01 00 00 34 13 00 00 16 00 00 00 98 00 00 00 20 15 00 00	.....h.....$. ..... $.....`... ....8.....T..... ..,.....4..... ...	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.4.0.4.<./.P.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 36 00 37 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.9.6.7.8.<./.U.p.t.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 35 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.5.9.3.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.5.1.1.6.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 35 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.1.5.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 39 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.9.0.9.3.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 31 00 38 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.9.0.1.1.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.5.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.2.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 37 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.4.2.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 37 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.1.5.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 32 00 32 00 30 00 37 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.2.0.7.7.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.7.2.<./.P.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 36 00 31 00 38 00 35 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.7.6.1.8.5.8.<./.U.p.t.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 33 00 33 00 33 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.3.3.3.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 32 00 34 00 38 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.2.2.4.8.4.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 38 00 38 00 33 00 39 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.8.8.3.9.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 37 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.7.1.5.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 37 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.1.7.2.0.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.0.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.8.3.7.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 34 00 36 00 36 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.2.4.6.6.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 39 00 36 00 30 00 36 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.6.9.6.0.6.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 34 00 36 00 36 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.2.4.6.6.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.0.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.r.x.d.p.u.s.,. .I.n.c...</.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.r.x.d.p.u.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 35 00 32 00 31 00 35 00 37 00 39 00 34 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.1.5.7.9.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 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	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 31 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.1.5.Z.".>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 30 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 36 00 36 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 36 00 30 00 39 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.6.". .P.I.D.=.".6.4.0.4.". .U.p.t.i.m.e.M.S.=.".6.6.0.9. ". .T.i.m.e.S.i.n.c.e.C.r.e.a. t.i.o.n.M.S.=.".6.6.0.9.". .S. u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 35 00 39 00 64 00 36 00 65 00 61 00 66 00 2d 00 37 00 31 00 65 00 36 00 2d 00 34 00 61 00 32 00 39 00 2d 00 38 00 65 00 61 00 38 00 2d 00 32 00 30 00 32 00 31 00 65 00 63 00 32 00 35 00 33 00 65 00 32 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.5.9.d.6.e.a.f.-.7.1.e.6.-.4.a.2.9.-.8.e.a.8.-.2.0.2.1.e.c.2.5.3.e.2.e.<./.G.u.i.d.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 31 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.1.5.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF9B.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB133.tmp.xml	unknown	4597	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d\Report.wer	unknown	2	ff fe	..	success or wait	1	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	157	6DF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_7225963344ab2d4b76a392ee69fe603ad8f2abb_b4806494_1a50c15d\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 38 00 34 00 34 00 38 00 34 00 37 00 31 00 35 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.8.4.4.8.4.7.1.5.4.	success or wait	1	6DF5497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{505b24ca-9a58-aba3-cdce-e230061e0c5c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 C4 E3 56 00 91 82 71 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 4A 0C 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DF71FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 7016 Parent PID: 6404

General

Start time:	07:16:24
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6404 -s 472
Imagebase:	0x240000
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	6FE81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp.xml	success or wait	1	6FE74BEF	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFA7.tmp.csv	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE267.tmp.txt	success or wait	1	6FE74BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 4a 32 10 60 a4 05 12 00 00 00 00 00	MDMP..... .....J2.`.....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 b8 15 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 04 19 00 00 35 32 10 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B..... ..GenuineIntelW.....T... .....52.`..... .....0..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6c ef 56 00 00 00 00 00 00 00 00 00 fb 75 00 00 1c 23 00 00 00 00 00 00 00 00 00 00 91 82 71 00 23 00 00 00 46 02 01 00 34 ef 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...l.V..........u...#...... ......q.#...F...4.V.+.........	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	168	08 19 00 00 00 00 00 00 05 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 91 82 71 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 f0 18 00 00	..........................q... ....<...........	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	20	0d 00 00 00 00 90 39 00 00 00 00 00 98 04 00 00 f4 24 00 00	......9..........$..	success or wait	13	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 05 01 a0 7b ad 77 48 17 87 00 00 00 00 00 00 00 87 00 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 41 00 00 00 00 00 f8 7b ad 77 ff 07 01 00 00 00 00 00 00 00 11 7f 00 00 00 00 30 07 11 7f 00 00 21 7f 28 02 22 7f 50 06 23 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	............{.wH...........y .w...............t..........A...... {.w................0.....!. (.".P.#.................m........ ....`f.w.. ....PS.w.........B......	success or wait	12	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	256	24 40 52 51 e8 72 f9 00 00 c7 44 24 38 b7 fc 00 00 8d 7c 24 3c 33 c0 83 c4 10 ab 33 f6 ab ab c7 44 24 10 26 99 00 00 c1 6c 24 10 09 c1 64 24 10 10 81 74 24 10 7c 47 41 df 81 74 24 10 12 34 0d df c7 44 24 14 ab 5b 00 00 c1 6c 24 14 06 c1 64 24 14 05 81 74 24 14 1b 6c 00 00 c7 44 24 40 e3 21 00 00 c1 64 24 40 03 81 44 24 40 b4 19 ff ff 81 4c 24 40 75 c0 62 af 81 74 24 40 fd e8 62 af 8b 45 3c 8b 7c 24 40 89 44 24 24 8b 5c 28 78 03 dd 8b 43 1c 8b 4b 20 03 c5 89 44 24 20 03 cd 8b 43 24 03 c5 89 4c 24 18 89 44 24 1c eb 24 8b 04 b9 8b 54 24 14 03 c5 8b 4c 24 10 50 e8 c9 34 00 00 35 04 34 01 5f 59 3b 44 24 3c 74 0c 8b 4c 24 18 47 3b 7b 18 72 d7 eb 2c 8b 44 24 1c 8b 74 24 20 0f b7 04 78 8b 34 86 03 f5 3b f3 72 17 8b 44 24 24 8b 44 28 7c 03 c3 3b f0 73 09 8b ce e8	$@RQ.r....D$8.....\|$<3.....3 .. ..D$.&....l$...d$...t$.|GA..t$ ..4...D$..[...l$...d$...t$..l. ..D$@.!...d$@..D$@.....L$ @u.b. .t$@..b..E<.\|$@.D$$.\ (x...C..K ...D$ ...C$...L$..D$..$....T$ ....L$.P..4..5.4._Y;D$<t..L$ .G;{.r..,.D$..t$ ...x.4...;.r..D $$.D(|..;.s....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6c ef 56 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 91 82 71 00 23 00 00 00 46 02 01 00 34 ef 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...l.V.................... ......q.#...F...4.V.+.........	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	48	1c 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 3a 00 00 00 00 00 e0 f9 b6 00 00 00 00 00 20 06 00 00 5c 6a 00 00 cc 02 00 00 54 21 00 00	.... :............ ...\j......T!..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	4	1b 00 00 00	....	success or wait	27	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	27	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	120	00 00 d5 74 00 00 00 00 00 40 14 00 48 78 14 00 ad 9a 07 f5 b6 18 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 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 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	...t.....@..Hx................ ....B.......B?........... ...."............ ..@A.........................	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	34	1c 00 00 00 42 00 73 00 59 00 48 00 78 00 65 00 58 00 37 00 4f 00 6b 00 2e 00 64 00 6c 00 6c 00 00 00	....B.s.Y.H.x.e.X.7.O.k...d.l.l...	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	668	00 00 71 00 00 00 00 00 00 00 d0 09 00 00 00 00 00 00 19 5e 42 2a ce 18 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 04 00 00 00 00 30 09 02 00 00 00 00 00 50 b2 02 00 00 00 00 3e 4d 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 ae fe 00 00 00 00 00 00 50 58 03 00 00 00 00 00 1c 6f 02 00 00 00 00 00 b3 1b 0c 00 00 00 00 00 8d e3 13 00 00 00 00 00 40 ff 1f 00 00 00 00 00 e6 08 14 00 00 00 00 00 c0 d5 f4 51 00 00 00 00 ce 75 3c 16 00 00 00 00 dc 87 17 0d 00 00 00 00 2d b0 e8 00 00 00 00 00 18 99 00 00 df bb 00 00 11 7b 04 00 ca cb 01 00 8d e3 13 00 d1 af 17 00 e6 08 14 00 16 83 2f 00 f9 23 01 00 f1 45 0f 00 00 00 00 00 37 d0 1f 00 d6 59 04	..q.....^B*.....Zb ....0.....P .....>M..... ....PX.....o..... .....@.....Q.... .u<.....-..... {...../..#.. .E.....7....Y.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	6784	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 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	....F.i.l.e.....F.i.l.e..... ..F.i.l.e.....F.i.l.e..... E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BE.tmp.dmp	unknown	120	03 00 00 00 94 00 00 00 08 07 00 00 04 00 00 00 68 0b 00 00 a8 07 00 00 0e 00 00 00 24 00 00 00 10 13 00 00 05 00 00 00 d4 00 00 00 20 24 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 68 11 00 00 5c 83 00 00 15 00 00 00 ec 01 00 00 34 13 00 00 16 00 00 00 98 00 00 00 20 15 00 00	................h.....$. ..... $.....`... ....8.....T.....h. ..\.....4..... ...	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.4.0.4.<./.P.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 32 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.1.2.8.7.<./.U.p.t.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 35 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.5.9.3.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 36 00 30 00 35 00 34 00 37 00 30 00 37 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	<.V.i.r.t.u.a.l.S.i.z.e.>.6.0.5.4.7.0.7.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 31 00 35 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.1.5.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 39 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.9.0.9.3.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.9.0.5.2.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.5.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 31 00 32 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.2.2.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 39 00 32 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.2.0.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.0.6.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 32 00 32 00 30 00 37 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.2.0.7.7.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 32 00 31 00 39 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.1.9.9.5.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.7.2.<./.P.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 37 00 33 00 34 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.7.7.3.4.6.7.<./.U.p.t.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4..g.u.e.s.t.=.".0.".h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 33 00 33 00 33 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.3.3.3.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 32 00 34 00 38 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.2.2.4.8.4.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 35 00 32 00 36 00 33 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.6.5.2.6.3.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 37 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.7.1.5.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.1.1.9.8.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.0.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 37 00 35 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.7.5.6.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 32 00 38 00 36 00 36 00 37 00 39 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.8.6.6.7.9.0.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 39 00 36 00 30 00 36 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.6.9.6.0.6.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 32 00 38 00 36 00 36 00 37 00 39 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.8.6.6.7.9.0.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.0.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.r.x.d.p.u.s.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 72 00 78 00 64 00 70 00 75 00 73 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.r.x.d.p.u.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 35 00 32 00 31 00 35 00 37 00 39 00 34 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.1.5.7.9.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.8.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 32 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.2.7.Z.".>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 30 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 36 00 36 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 36 00 30 00 39 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.6.". .P.I.D.=.".6.4.0.4.". .U.p.t.i.m.e.M.S.=.".6.6.0.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".6.6.0.9.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 39 00 31 00 64 00 66 00 61 00 63 00 63 00 2d 00 31 00 33 00 63 00 61 00 2d 00 34 00 64 00 65 00 31 00 2d 00 62 00 34 00 31 00 37 00 2d 00 35 00 65 00 62 00 32 00 64 00 63 00 35 00 66 00 30 00 31 00 35 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.9.1.d.f.a.c.c.-.1.3.c.a.-.4.d.e.1.-.b.4.1.7.-.5.e.b.2.d.c.5.f.0.1.5.e.<./.G.u.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 35 00 3a 00 31 00 36 00 3a 00 32 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.2.6.T.1.5.:.1.6.:.2.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD04.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF96.tmp.xml	unknown	4557	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63\Report.wer	unknown	2	ff fe	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	157	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_loaddll32.exe_c5a25cdcc8f97dcd0e408681553972f33acea_b4806494_1b20ef63\Report.wer	unknown	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 31 00 39 00 38 00 34 00 36 00 30 00 38 00 37 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.9.8.4.6.0.8.7.8.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b8671b95-6da2-6119-c4c8-6c2b87ccc673}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 4A 0C 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 91 82 71 00 02 00 00 00 00 00 00 00 3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6FE91FE8	RegSetValueExW

Disassembly

Code Analysis