ID: 385485
Sample Name: utility.dll
Cookbook: default.jbs
Time: 15:26:29
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

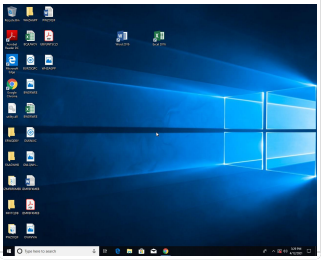
Analysis Report utility.dll

Overview

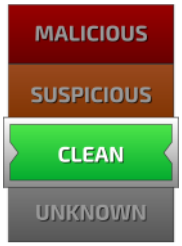
General Information

Sample Name:	utility.dll
Analysis ID:	385485
MD5:	c84fd1069470c4f..
SHA1:	94ca6af9cae3367..
SHA256:	59d2ed9608ac54..
Infos:	

Most interesting Screenshot:



Detection

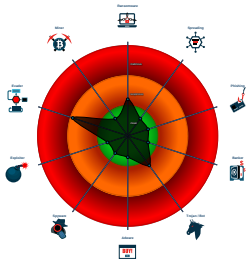


Score:	8
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to access load…
- Contains functionality to dynamically…
- Contains functionality to open a port…
- Contains functionality to query netwo…
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function
- Extensive use of GetProcAddress (o…
- Found large amount of non-executed…
- Monitors certain registry keys / valu…
- One or more processes crash

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6788 cmdline: loaddll32.exe 'C:\Users\user\Desktop\utility.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6836 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6880 cmdline: rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 7020 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 696 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6868 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,CPUSpeed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7060 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6868 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7124 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6080 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 3492 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt2BinStr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4544 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3492 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4264 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DecryptEx MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6384 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Deflate MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6528 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DeflateToMemory MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6656 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawEnumDisplayModes MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6136 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawIsSupported MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6308 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawRestoreDisplayMode MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4108 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawSetDisplayMode MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6096 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryAdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4612 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6096 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6672 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryClear MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7064 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryDump MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

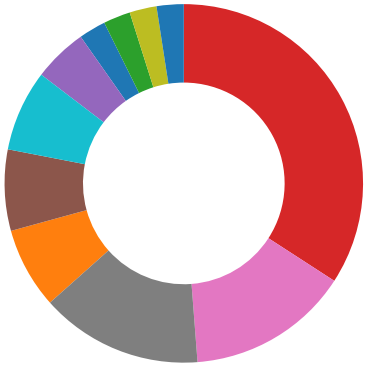
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Cryptography
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Remote Access Functionality

Click to jump to signature section

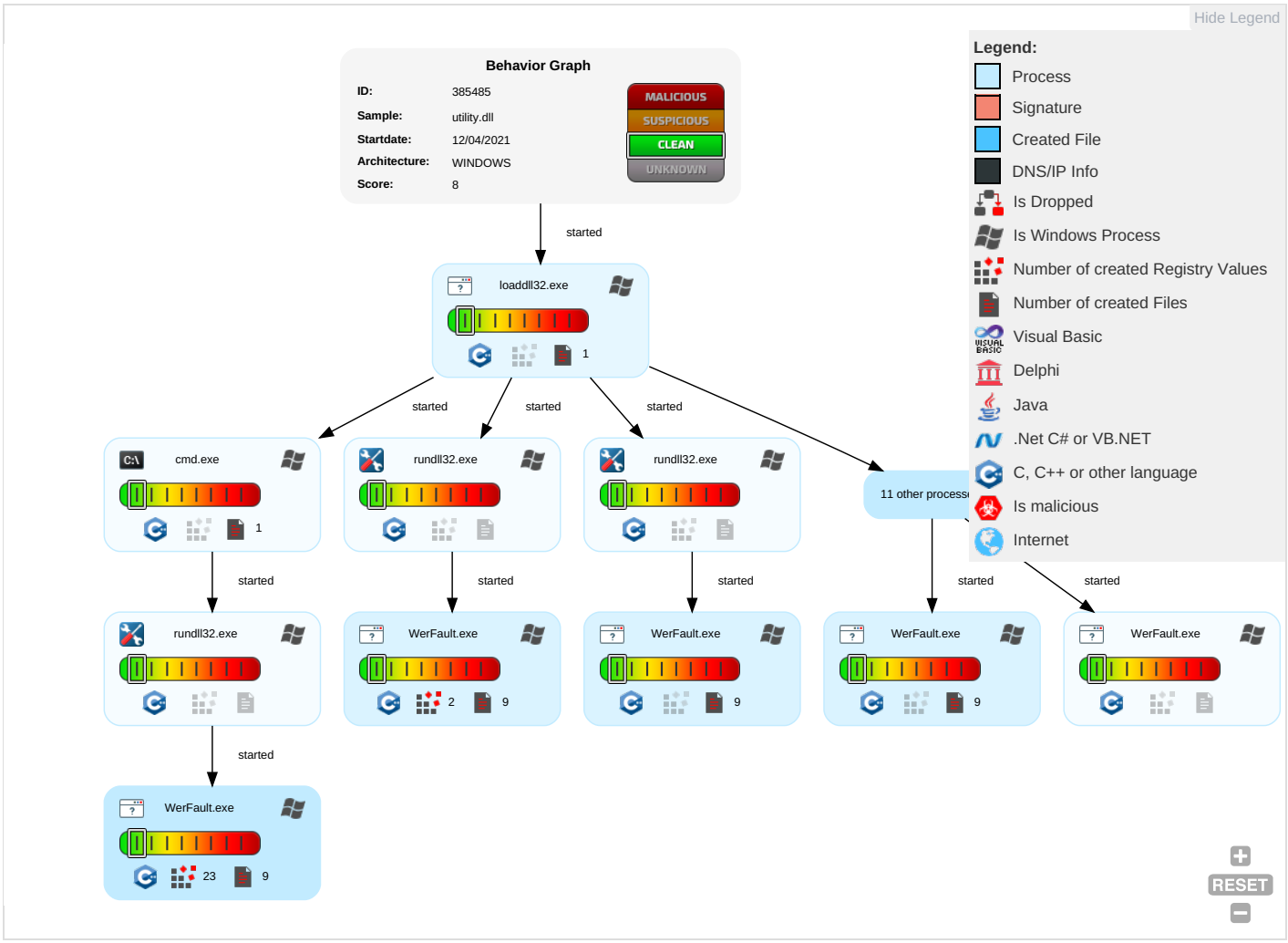
There are no malicious signatures, click here to show all signatures.

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	Native API 1	Application Shimming 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 1 1	LSASS Memory	Query Registry 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)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 3 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)	Rundll32 1	NTDS	Virtualization/Sandbox Evasion 1 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	Remote System 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	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

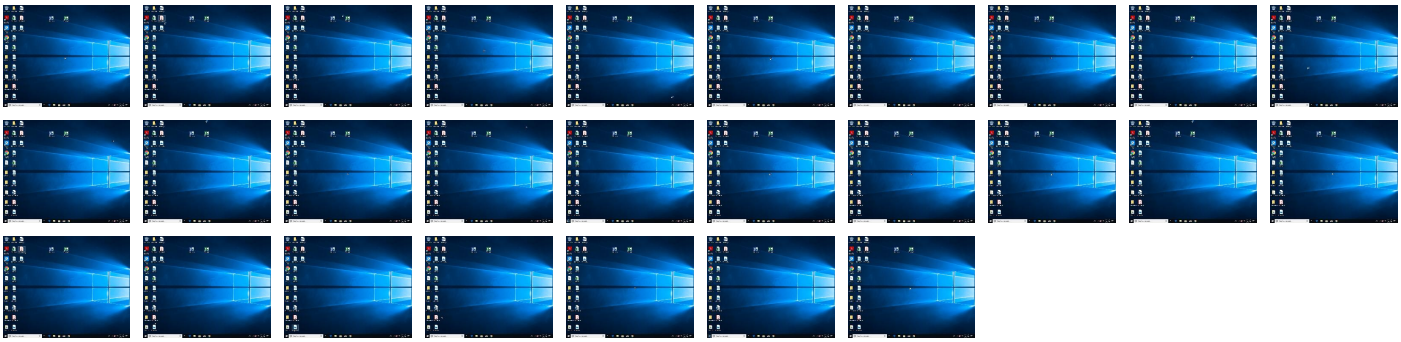
Behavior Graph



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
utility.dll	0%	Virustotal		Browse
utility.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.m	0%	URL Reputation	safe	
http://microsoft.coA	0%	Avira URL Cloud	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.micro(	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://crl.microsy	0%	Avira URL Cloud	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://crl.microsoft2	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.m	WerFault.exe, 0000000E.00000003.749476068.000000000502A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://microsoft.coA	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micro	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	utility.dll	false		high
http://https://www.thawte.com/cps0/	utility.dll	false		high
http://crl.microsoft	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.micro(	WerFault.exe, 0000000B.00000003.676315749.00000000049D4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ocsp.thawte.com0	utility.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsoft.co	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsy	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.thawte.com/repository0	utility.dll	false		high
http://www.microsoft.c	WerFault.exe, 00000023.00000002.762386513.0000000005250000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsoft2	WerFault.exe, 00000009.00000003.683820033.0000000004D79000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385485
Start date:	12.04.2021
Start time:	15:26:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	utility.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:	40
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:	CLEAN
Classification:	clean8.winDLL@48/20@0/0
EGA Information:	• Successful, ratio: 25%
HDC Information:	• Successful, ratio: 100% (good quality ratio 96%) • Quality average: 85% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.88.21.125, 40.88.32.150, 104.43.139.144, 104.43.193.48, 20.82.210.154, 92.122.213.194, 92.122.213.247, 20.190.160.74, 20.190.160.131, 20.190.160.7, 20.190.160.1, 20.190.160.70, 20.190.160.133, 20.190.160.3, 20.190.160.130, 52.147.198.201, 20.190.160.9, 20.190.160.72, 20.190.160.5, 20.190.160.135, 2.20.142.209, 2.20.142.210, 20.190.159.137, 40.126.31.2, 20.190.159.133, 40.126.31.142, 20.190.159.131, 20.190.159.135, 40.126.31.140, 40.126.31.3, 52.155.217.156, 52.255.188.83, 20.54.26.129, 168.61.161.212 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Execution Graph export aborted for target rundll32.exe, PID 6384 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 6528 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
15:27:30	API Interceptor	5x Sleep call for process: WerFault.exe modified
15:28:21	API Interceptor	1x Sleep call for process: loaddll32.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_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12320
Entropy (8bit):	3.7664906162615877
Encrypted:	false
SSDEEP:	192:11HpiB0oXRR+HBUZMX4jed+h+/u7sfS274ItWcY:/JivXGBUZMX4jes+/u7sfX4ItWcY
MD5:	CA7808A969BB6ECE94BE53CA5EB5815A
SHA1:	2282A52F119D8DCCA59EA920B602899092486B97
SHA-256:	F14D3D718B6921058C178C26BE5564A149A64B9FB53C755E8F73BAB09328D3CB
SHA-512:	181CBDF4D245E1E9CA7ED3835C8677B9F5F1F681422B3501F23C2F924BE74870A30970B94529D36C578B8B92291A31709C9EFB825806EFE38B0BFB2B76F9A79C
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.6.3.9.3.0.8.1.2.5.5.....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.=.1.3.2.6.2.7.0.7.6.4.7.9.0.1.8.5.1.6.....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.=.9.d.9.4.b.c.d.8.-.7.0.6.e.-.4.b.9.1.-.9.3.6.0.-.d.2.5.6.2.1.1.f.7.5.0.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.2.6.2.9.3.3.2.-.d.9.f.8.-.4.a.6.0.-.9.c.f.2.-.b.f.9.2.3.2.d.1.1.3.d.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.0.-.0.0.0.1.-.0.0.1.b.-.e.2.d.7.-.a.a.8.d.9.f.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7679896352891276
Encrypted:	false
SSDEEP:	192:6ThGis0oX6R+HBUZMX4jed+h+/u7sfS274ItWcr:ohGiqX9BUZMX4jes+/u7sfX4ItWcr
MD5:	A383E5C2B05E613C4464C290EC341A21
SHA1:	6CDBC5CBC31CB08521FEBD43A382AC4046E7FBE5
SHA-256:	16179FB8445E44C464816421FE5B15CDE3B8A3BC9C226E6F3AB0F56311427811
SHA-512:	2DCC96E330B959B522C621324F1EA78ECEB1A312D1F8F556A260F191994F37C61B6B961F6383DDD066FDCEE3B6B094AC29FB85934139BAC745347D0E7FB95AD
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.6.3.9.1.9.8.7.4.9.9.....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.=.1.3.2.6.2.7.0.7.6.4.8.0.8.9.3.4.4.5.....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.=.1.c.4.8.7.3.6.6.-.f.c.8.a.-.4.f.a.e.-.b.9.7.6.-.1.f.3.5.4.6.f.4.9.f.3.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.e.1.e.b.7.0.b.-.6.e.f.9.-.4.0.4.9.-.b.6.1.1.-.3.4.8.d.0.6.c.f.f.9.5.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.d.4.-.0.0.0.1.-.0.0.1.b.-.8.f.7.2.-.a.6.8.d.9.f.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6995fa83d7b0318a43db0d33e1e8ff1c3499353_82810a17_12577480\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6995fa83d7b0318a43db0d33e1e8ff1c3499353_82810a17_12577480\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12318
Entropy (8bit):	3.766194179464847
Encrypted:	false
SSDEEP:	192:cfiB0oXDHBUZMX4jed+h+/u7sfS274ItWcc:sivXDBUZMX4jec+/u7sfX4ItWcc
MD5:	52E712DC29F2F6F344AD9416CBF531FB
SHA1:	9C3F9F4564C154100025A9DB1448D61BB65F791E
SHA-256:	649A67169BE17298E22BB527798F8B0C0568E681BE3DF9359E066F702A4FF4D3
SHA-512:	0A5077FDAD198AE8FC68BB4143FFF82F421E10FDA4D474DB381BE335AC2BC0FACED81A69FE27D3C8D71B3F7A91DAFF0F53D8BED6729D16618F5E49F9F09A72C9
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.6.7.4.5.7.3.6.5.3.1.....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.=.1.3.2.6.2.7.0.7.6.8.4.8.8.6.0.9.9.1.....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.f.c.4.2.f.2.2.-.1.4.f.c.-.4.e.a.b.-.a.e.0.3.-.1.9.b.a.2.9.6.8.f.8.3.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.d.c.6.a.a.b.5.-.d.2.b.7.-.4.3.f.8.-.8.a.4.a.-.0.c.a.4.4.a.e.9.4.e.6.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.d.0.-.0.0.0.1.-.0.0.1.b.-.e.9.a.8.-.d.f.a.1.9.f.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_11932288\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12322
Entropy (8bit):	3.7683657592986455
Encrypted:	false
SSDEEP:	192:B52ih0oXvqHBUZMX4jed+h+/u7sfS274ItWcQ:OiPX6BUZMX4jec+/u7sfX4ItWcQ
MD5:	A8CD37436DD55291AEFE3DE38A97E230
SHA1:	D637BBC284DE9B0D05BE24FAFF29C3060303B28B
SHA-256:	A015EEA577F7F4100C025C92235B0BDCC297C59281A55ABA46ED076B2EE7A846
SHA-512:	C2D49CCF4DCE04D067138357721DDA7404DEB06E9044EE863E47FD0CD148F5A21FD335CB31196C2603F94A7341196C6807F8D75512D28BE52F7AA271C9C38F8
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.6.4.7.2.4.5.5.9.7.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.7.0.7.6.6.2.2.9.2.4.2.5.2.....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.=.1.d.0.7.1.6.c.3.-.6.b.6.6.-.4.c.7.c.-.b.3.1.c.-.8.5.a.0.5.8.2.f.2.3.f.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.2.a.0.c.4.4.2.-.8.d.f.3.-.4.f.2.6.-.8.9.6.c.-.9.7.1.8.5.e.3.0.7.5.2.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.a.4.-.0.0.0.1.-.0.0.1.b.-.a.7.4.7.-.8.9.9.1.9.f.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_17936916\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12318
Entropy (8bit):	3.7670207117332146
Encrypted:	false
SSDEEP:	192:Ml/iS0oXSqHBUZMX4jed+h+/u7sfS274ItWc1:a/i0X3BUZMX4jec+/u7sfX4ItWc1
MD5:	31FA4DC2FECF09081F39561EE652E953
SHA1:	2CE0ECF0B4051A4718E76D64EB06154F8E2DFB09
SHA-256:	76C679665E76B0E15C4F8472855029F4C01FAF5F6E9A3A0D2497461D42CE92B7
SHA-512:	11265072313C191AB6DFE7F2BD01157B3E0C5264D986D674535A995157BCECBD3910DDD53A7F622B972E3EAF4C94AFC866CDB231C66D11C3CBACC7D6750B6FA
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.6.4.2.4.0.1.8.6.5.1.....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.=.1.3.2.6.2.7.0.7.6.5.7.6.5.1.8.1.9.9.....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.=.8.2.b.8.9.b.3.e.-.5.1.d.e.-.4.a.e.4.-.a.4.c.0.-.2.f.a.9.5.6.f.2.f.d.3.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.a.a.2.4.1.a.1.-.0.3.e.7.-.4.5.3.c.-.b.d.8.6.-.b.4.9.4.6.1.5.d.4.3.3.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.d.4.-.0.0.0.1.-.0.0.1.b.-.f.e.2.4.-.9.7.8.f.9.f.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER440A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 13:27:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45576

C:\ProgramData\Microsoft\Windows\WER\Temp\WER440A.tmp.dmp	
Entropy (8bit):	2.114361418312875
Encrypted:	false
SSDEEP:	192:ByTnPmJD/WCsMq7J3dDlWia7rrLQ4LKO0Get7HPPWfJsYC3bLs:QnY7/q7XpWiuDlLhedPPWRsYyE
MD5:	BC29969592FCE61CC7307FB86A9A16CC
SHA1:	F8A02FE31E154F32A7D780A00D170F16E35C6A18
SHA-256:	9CE619DF22EB50415DFBB646A1893F6B1AC49DD210BBDC6E64C46DF538B038C9
SHA-512:	47B25E4E3A77B7B1DE8F1884037FECA8F6F71E0DD6721E634B7CC7B72EFF08179579704CE93BB67D6DF6C4C468F993167AB13EF6A9FEF42B2A0AB5E43C95EC 1
Malicious:	false
Preview:	MDMP..... .....Jt`.....U.....B.....<.....GenuineIntelW.....T.....Jt`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....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\WER5001.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):	8254
Entropy (8bit):	3.6925255797972847
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUE6R6Y7U6ngmfTgS3a+pra89bvREGqsfcVBm:RrlsNin6R6Yl6ngmfTgS3lvREGJfC8
MD5:	A54AF6B0E5BE70F66D1364DFEA66E293
SHA1:	3E7C61679DAE3534C7844A2533E25CFFAC6DACDC
SHA-256:	BB5915E893B211C8C3EDAAABBFF410E54B37C53B7E478CC45410C900BE324D8F
SHA-512:	00F6429A03CD2C6099FCFF6CF79AF6AA1E73EC19740E2A89330399B559564CFB2B0014B3345B8EA6FF7F993985D6131F5F3440A107E33BB17F233F5EED9444D2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.9.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER54A6.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.452465742872191
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9CAu9kWSC8BW8fm8M4JCds8F4ak+q8/pLJ4SrS8d:ulTfUfAu99SNJJwkYJDW8d
MD5:	D31D6603740CE9CE6E0E696F86C22AC4
SHA1:	7AF324A5773DA231069ED96BB9301F1F9DDD1155
SHA-256:	D59E15291C5CDF0772FC20438B3A9B60730352A743F119A400A778B54FEFE044
SHA-512:	A21CC9C358CF1A676E433BEC513B409668CF52F4073794B535F90F401D08EA39D83E2B7BD288BD7C9B0F83115FA7ED3C392BF4B79A08336BDA0679C9E04E5A0 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943118" />.. <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\WERBA0A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 13:27:21 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46500
Entropy (8bit):	2.0966181040226965
Encrypted:	false
SSDEEP:	192:wlUSxE+xIQgPV9wlTwENLdfjT45LQ4LKO0GeC/3lEDzAWgnCIF:ALPSRaGQT45lLheSVEuNF
MD5:	B5E76FE7CE8FD6D4307D1853FAF2F6DB
SHA1:	64981726DF130BE566D82F82A8187D66E1326FAD
SHA-256:	D86783105B9E35139FD4804CA936F773D19DADD0B5D86A8237407C779C79E01E

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	
SHA-512:	EED406B29F0E29578C90FB01A8EDD1C51D4ABBE08806E40AE79E037344501A0C56F6FEE7316D53FE494C0A6298CDEAD45F8F762F3FD0D433C1EB5FEC7D18DF61
Malicious:	false
Preview:	MDMP..... .....Jt`.....U.....B.....<.....GenuineIntelW.....T.....Jt`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WERBA48.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 13:27:21 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44412
Entropy (8bit):	2.2018242460678756
Encrypted:	false
SSDEEP:	192:sJmCXdwHi3rJvRqWOtv/w+u3IntdnLQ4LKO0Ge9ikzSWZ3y0nlA:cftAI1pT3IHlLheAkzSa3Ju
MD5:	AF8F54F2D8735827C37F794B96787A7D
SHA1:	1CEAC03031CE26BFB9B6451D7D6A5D698BF9ADDF
SHA-256:	1E649645DCB02410D73B927846BCEB7AE95060E4121AC7BBCCF413497E2F4B44
SHA-512:	C010C35DD9612BF64F41BD93D188B83CBDD7E0D0F4CB737DE37E3B36EE31ECCACC36C9A783A41A4A54E016BFB9968936EAC7F89D54BF8FA87869B3313D9960A
Malicious:	false
Preview:	MDMP..... .....Jt`.....U.....B.....<.....GenuineIntelW.....T.....Jt`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WERC277.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):	8246
Entropy (8bit):	3.692815470892518
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNid8l6G6Y7b6T+gmfT5S3a+prx89bvgRsfXJVGm:RrlsNi26G6YH6qgmfT5S3YvgKfXLv
MD5:	EFF0134F045E46E1192474917C62C2A8
SHA1:	150210F8BEB107014D03BDA39C6E8B0096387AD2
SHA-256:	9DFC6C18094C27F0FABA373C78BCFB8766F8A5885C9BA29CAA2CC8BEB849E0C3
SHA-512:	79DCA8F941CEF2EC8B764CBC643DA37AF167FCD1D1E34F899621EFE0812B2CA1A11B34A8B4ED33C1741BCEAE2A9582CDF19D42FFF30CC9A3AD1347123F114D8
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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):	8242
Entropy (8bit):	3.6949087264063945
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLz6N6YQNy6SgmfT5S3a+prC89bvgwsfxyVGm:RrlsNif6N6YQo6SgmfT5S3dvgDfx8v
MD5:	F12BE363E51A81F887EDF21839B285DA
SHA1:	DCE576D1D5A11D26C281DB1092F333D67027EF24
SHA-256:	BFFA931F6988EA1764084F5CB096E5B288691EF577D409C85D0E1DDCA59D07F2
SHA-512:	E38C2A93DA773DF57917C25A3831963D1B417B611069017AB756014CA4A9AFCCA2767ACBCF898C16B4DE21592ABA7351A99782415993ED790E66BACA624E73E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	
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.>.6.8.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.457170834098322
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9CAu9kWSC8B7a8fm8M4JCdsHF7C+q8/pz4SrSkd:uITfUfAu99SNBvJSWDWkd
MD5:	699CC41587F86CAD1446EB8EA973833D
SHA1:	98EE477D0D7862B1CCB2E345D874856F147979F2
SHA-256:	B503E7817E567D1269EA282A68A19C9B4A851F24F490382A4C3617326ABC6B73
SHA-512:	EAA33FA55C1E06D3EDFEA65867E26480D3B1B3182CF84911B7ACD0A8B00A68FF3F8658ED53505063E434F552083FCFC64979814A4317FEA3501EA7689A8C1D60
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943118" />.. <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\WERC65E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 13:27:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49520
Entropy (8bit):	2.3362085739645937
Encrypted:	false
SSDEEP:	192:O6siwtXlAB2U2cZ+0p0AMEiitHIoI0bLZHXLQ4LKO0GeQSEyPslknkb7:uiwtS2E+c0ZViH7lLheCyPsOkb7
MD5:	44CC6081D6CB80DF9AE9CEF179A6218A
SHA1:	17E065CBF0150334085C49E28EB92C5C41568281
SHA-256:	4AA10C796CA9DCAAF06F7A142C6E6EEE15B282A900D3D7D1E6FA2D5290010D7B
SHA-512:	41FB82BBE4E549612C59D2C4F95461EF198ABFA105C8995E41B161D1C7453EEC05ABDE090786D1331CC616DB116814FBEB5762192E6FA7C7FF700C421744F3FA
Malicious:	false
Preview:	MDMP..... .....Jt`.....U.....B.....<.....GenuineIntelW.....T.....Jt`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WERC68F.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.455212563263293
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9CAu9kWSC8BVa8fm8M4JCdsHFnbm+q8/pA4SrS5d:uITfUfAu99SNbvJDaRDW5d
MD5:	10F58E17A07F4E81B4A09BDB9E4483A1
SHA1:	6F19E9FCA58A6FE6B2D35C6B7870B524947760A6
SHA-256:	CDF44C3800A39E385C92BCA66A0C63439EE9421FA94A676AFC799CAD18C85DB8
SHA-512:	DAF7FA0F820EECE74DEE426F7B43F21E8C6240655ECCF8A801225983B31D64D36E19D77CF6D33B1CDCAF5DF3DA434CED0BF5C210F1D96A872DF9CCA540BD1D7
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943118" />.. <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\WERD4A7.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):	8262
Entropy (8bit):	3.693477261844468
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNil26s6Y7X56h+gmfT9S3a+pr089bv/asfvVvm:RrlsNiU6s6YD564gmfT9S33v/5ftO
MD5:	E499F2C76629836DBE1245A34BDC675B
SHA1:	D89C46F462AB2B12F286630D314EFFFB31B2536A
SHA-256:	7AC2E35783203637A969C6C3884A338C319B9E7B81D3150176EDE53CAA47EDA5
SHA-512:	8841073B5DDA7A8672A934A68CEA428FAF9BF01AD2E8A74DC35144AEBE356D43546F363E156CD73C273596294C642E4CE318218FA758B67220CD9FC4142FE9E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 13:27:33 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49112
Entropy (8bit):	2.3871068415769936
Encrypted:	false
SSDEEP:	192:L61unKtaaoL9Yy9R711PCe5PubwyA15PerEZfh96ceUEtLQ4LKO0Ge6o/Es8Uavu:21unKtm57119kA1ZUsTEVlLheth8/KR
MD5:	FF37B9362F711225B025C77558F322E6
SHA1:	DEF70241888A46D351941386D4DB89BB4F89DD94
SHA-256:	29B952E4749C3A2250F6C9BEDC86CF541E2C8E986F746334917C1B239EBA995D
SHA-512:	D0BC54E0D9AF94639E2C45A6AB5691230B881ABD3D514E7E7EB4E8A390C704C1C1CBD5FC0487B5EB1D8FBDB11E8B54AE956F866E97007DBD524EA75C22814F5
Malicious:	false
Preview:	MDMP..... .....Jt`.....U.....B.....<.....GenuineIntelW.....T.....Jt`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WERDA46.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.455873668706281
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9CAu9kWSC8Bz8fm8M4JCdszFM3o+q8/pX4SrSDd:uITfUfAu99SNGJsoaDWDd
MD5:	81BD8600CF33BA0CEBA52C9044BF5CBD
SHA1:	A29C85A9ABF035708DC3A87C8B7D1FC18449DD38
SHA-256:	91F66D129E2D66868908101BC39123E91FBD470A1D17C96C57BB6E8FFFA9D8D2
SHA-512:	3012A84D1F0FDC1A4B47C0BF7AEB7E47DE936A961AE0BCC355D9EB039B2D033FD63B216D6D324D32BABC60E60FB303137EB39FD159303743AB61C9027F579FA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943118" />.. <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\WERF2DE.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):	8266
Entropy (8bit):	3.6920657312157865
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNiRW6TA6Y7h6ai+gmfT9S3a+pre89bvc5sf9mVam:RrlsNiw606Yd6abgmfT9S3RvcSfur
MD5:	8465DB4319C6F16F21998A5B1003D154
SHA1:	306148AF3F82C2A7CB8FE4039F7D7B3A32004A20
SHA-256:	2412CB9E17C290D6C7D8FBBF079618E9222C58824469AE796ED52965A205175C
SHA-512:	D6D1EC05B049239F1F861E0A9375ED94D5B3CC6B4084D5743D1B55522096C42C879DB3E1693FE7FDBAA4CD1E999972275C6F9E3B93A655E202216CCF8BC94D E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. </.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. </.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.4.9.2.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.456770616078265
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9CAu9kWSC8BJb8fm8M4JCdszF00+q8/pA4SrS8d:uITfUfAu99SN8JE0hDW8d
MD5:	DFDD032CDB874D482D455C803BE70853
SHA1:	C10B9EF458D0E6EDD93C4199DAEAE304D989432A
SHA-256:	29DEDB49059C487BFA7922710252B7842B1DF53B93F5262C835F08E2A59A064C
SHA-512:	287E90FBE5F63F5BF4850BB4298A90F9C1D9FD073196A98901865821D5B462D1FB0109C42E11AE27718D32B82277DA7A3186A70A03C25B49C28CFAAEF05A10EC
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943118" />.. <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 Wi ndows
Entropy (8bit):	6.246113418766052
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 98.32% • Windows Screen Saver (13104/52) 1.29% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	utility.dll
File size:	194296
MD5:	c84fd1069470c4f7cbcd9fa10fc32615
SHA1:	94ca6af9cae336754da47e2b8694a1f33db78e89
SHA256:	59d2ed9608ac543bd671da7b17558ebce275f64dd80fc84 abd10fd31dea49c5e
SHA512:	f37f6eaf9f234fbe93619c72e7e012fb37b6b5779ff80c244f c19bd3bb628b0193d275c3e7f21d168fcb0f994a49c6116 9b11fde30819543092d09b41283903d
SSDEEP:	3072:+KEDvFkRNFycul5xjfMEOlL9M0Uiu+SeiMEvqrW B37d7YM1t7OrGsLZQm:2vF1fIL9M0UiuheZEyrWBrhY MzOrGOT
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....>.@A_i. A_i.A_i..}b.C_i.:Ce.@_i..Cg.W_i..@c.4_i..@b.K_i.A_i.K_ i.A_h._i..P4.P_i.G|c.C_i.G|b.Z_i...m.@_i.RichA_i..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001782f
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x55C07E95 [Tue Aug 4 08:57:57 2015 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:	f57837ddefd6a23c92486b80aca0917a

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=thawte SHA256 Code Signing CA, O="thawte, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 5/4/2015 2:00:00 AM 5/8/2016 1:59:59 AM
Subject Chain	• CN=Northcode Inc., OU=SECURE APPLICATION DEVELOPMENT, O=Northcode Inc., L=Ottawa, S=Ontario, C=CA
Version:	3
Thumbprint MD5:	C53B59F35C5767ABA434E5064C15AB35
Thumbprint SHA-1:	AB6E9D1997F370BB16124928C4817BBC196BE3FA
Thumbprint SHA-256:	653E2B5E0DC1BBD9E0696457D74C4CADF306AEB7BC8AE16B0CD9A15E9700605A
Serial:	7EFA7BCE3063E7499CE40F37454B10A6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ebx
mov ebx, dword ptr [ebp+08h]
push esi
mov esi, dword ptr [ebp+0Ch]
push edi
mov edi, dword ptr [ebp+10h]
test esi, esi
jne 00007F5100A106DBh
cmp dword ptr [1002ED14h], 00000000h
jmp 00007F5100A106F8h
cmp esi, 01h
je 00007F5100A106D7h
cmp esi, 02h
jne 00007F5100A106F4h
mov eax, dword ptr [1002F444h]
test eax, eax
je 00007F5100A106DBh
push edi
push esi
push ebx

Instruction
call eax
test eax, eax
je 00007F5100A106DEh
push edi
push esi
push ebx
call 00007F5100A105BCh
test eax, eax
jne 00007F5100A106D6h
xor eax, eax
jmp 00007F5100A10720h
push edi
push esi
push ebx
call 00007F51009FBDB6h
cmp esi, 01h
mov dword ptr [ebp+0Ch], eax
jne 00007F5100A106DEh
test eax, eax
jne 00007F5100A10709h
push edi
push eax
push ebx
call 00007F5100A10598h
test esi, esi
je 00007F5100A106D7h
cmp esi, 03h
jne 00007F5100A106F8h
push edi
push esi
push ebx
call 00007F5100A10587h
test eax, eax
jne 00007F5100A106D5h
and dword ptr [ebp+0Ch], eax
cmp dword ptr [ebp+0Ch], 00000000h
je 00007F5100A106E3h
mov eax, dword ptr [1002F444h]
test eax, eax
je 00007F5100A106DAh
push edi
push esi
push ebx
call eax
mov dword ptr [ebp+0Ch], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
pop esi
pop ebx
pop ebp
retn 000Ch
mov eax, dword ptr [1002ED20h]
cmp eax, 01h
je 00007F5100A106DFh
test eax, eax
jne 00007F5100A106E0h
cmp dword ptr [1002ED24h], 01h
jne 00007F5100A106D7h
call 00007F5100A14B12h
push dword ptr [esp+04h]
call 00007F5100A14B42h
push 000000FFh

Rich Headers

Programming Language:	• [LNK] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x24020	0xa3c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x231d8	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2e000	0x16f8	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x31000	0x16dc	.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	0x20000	0x2d0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1efe9	0x1f000	False	0.54097624748	data	6.67713038792	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x20000	0x4a5c	0x5000	False	0.51171875	data	5.97801634413	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x25000	0xb464	0x6000	False	0.198323567708	data	2.64122400209	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x31000	0x20ea	0x3000	False	0.399332682292	data	4.07308642566	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
USER32.dll	LoadCursorA, GetCursor, LoadImageA, UnregisterClassA, CreateWindowExA, RegisterClassA, DestroyWindow, DispatchMessageA, GetMessageA, PostMessageA, DefWindowProcA, GetWindowDC, OffsetRect, UnionRect, IntersectRect, ValidateRect, RedrawWindow, InvalidateRect, GetWindowLongA, SetWindowLongA, SetWindowRgn, GetDC, ReleaseDC, GetWindowRect, GetClientRect, ClientToScreen, SetRect, MessageBoxA, wsprintfA
KERNEL32.dll	CloseHandle, ReadFile, WriteFile, CreateFileA, GetFullPathNameA, DeleteFileA, LocalFree, LocalAlloc, GetFileSize, SetFilePointer, SetThreadPriority, GetThreadPriority, QueryPerformanceCounter, QueryPerformanceFrequency, GetCurrentThread, FreeLibrary, GetProcAddress, LoadLibraryA, GetLastError, SetFileAttributesA, GetFileAttributesA, lstrcpynA, lstrlenA, lstrcpyA, SystemTimeToFileTime, GetSystemTime, CompareFileTime, WideCharToMultiByte, MultiByteToWideChar, CreateThread, GetStringTypeW, GetTickCount, SetSystemTime, FileTimeToSystemTime, HeapFree, HeapAlloc, GetProcessHeap, GetVersion, GetStartupInfoA, GetCurrentProcess, GetModuleHandleA, SetLastError, GetVersionExA, CreateProcessA, GetStringTypeA, LCMapStringW, LCMapStringA, HeapSize, TerminateProcess, TlsGetValue, TlsFree, TlsAlloc, TlsSetValue, GetCurrentThreadId, ExitProcess, DeleteCriticalSection, InitializeCriticalSection, SetHandleCount, GetStdHandle, GetFileType, FreeEnvironmentStringsA, FreeEnvironmentStringsW, GetEnvironmentStrings, GetEnvironmentStringsW, SetUnhandledExceptionFilter, IsBadReadPtr, RaiseException, IsBadCodePtr, GetCPInfo, FlushFileBuffers, SetStdHandle, GetACP, GetOEMCP, CompareStringA, CompareStringW, SetEnvironmentVariableA, ExitThread, IsBadWritePtr, VirtualAlloc, VirtualFree, HeapCreate, HeapDestroy, GetEnvironmentVariableA, GetModuleFileNameA, GetCommandLineA, LeaveCriticalSection, EnterCriticalSection, GetLocalTime, RtlUnwind, HeapReAlloc, InterlockedDecrement, InterlockedIncrement, GetTimeZoneInformation
WSOCK32.dll	WSACleanup, listen, bind, htons, closesocket, WSAAsyncSelect, socket, WSAGetLastError, accept, recv, send, connect, gethostbyname, WSAStartup
GDI32.dll	GetObjectA, GetDIBits, OffsetRgn, BitBlt, DeleteDC, CreateCompatibleDC, SelectObject, ExtCreateRegion, CreateDIBSection, GetRegionData, CreateRectRgn, CombineRgn, DeleteObject, GetDeviceCaps
ADVAPI32.dll	RegCreateKeyExA, RegSetValueExA, RegOpenKeyExA, RegQueryValueExA, RegCloseKey, IsValidSid, EqualSid, GetSidSubAuthorityCount, GetSidLengthRequired, GetSidIdentifierAuthority, InitializeSid, GetSidSubAuthority, GetTokenInformation
ole32.dll	StgIsStorageFile, StgOpenStorage
OLEAUT32.dll	SysAllocString, SysStringByteLen, SysAllocStringByteLen, SysAllocStringLen, GetErrorInfo
NETAPI32.dll	NetUserModalsGet, NetApiBufferFree

Exports

Name	Ordinal	Address
CPUSpeed	1	0x100019d0

Name	Ordinal	Address
Decrypt	3	0x10001f10
Decrypt2BinStr	2	0x10001ff0
DecryptEx	4	0x10001eb0
Deflate	5	0x100013b0
DeflateToMemory	6	0x100018a0
DirectDrawEnumDisplayModes	7	0x100026b0
DirectDrawIsSupported	8	0x10002560
DirectDrawRestoreDisplayMode	9	0x10002650
DirectDrawSetDisplayMode	10	0x100025c0
DirectoryAdd	11	0x10002870
DirectoryClear	12	0x10002830
DirectoryDump	13	0x10002820
DirectoryLoadFile	15	0x10002a70
DirectoryLoadFile2	14	0x10002b80
DirectoryReadFileChunk	16	0x10002de0
DirectorySaveFile	17	0x10002e40
Encrypt	18	0x10001d30
EncryptEx	19	0x10001e50
FLAGetVersion	20	0x10003310
FLAOpenFile	21	0x10002f80
FileDecrypt	22	0x10002290
FileEncrypt	23	0x10002170
Hash	24	0x10001c00
Inflate	25	0x100013d0
InflateHeader	26	0x10001460
InflateHeaderFromBuffer	27	0x10001640
InflateToMemory	28	0x10001780
IsCursorARROW	29	0x100023e0
IsCursorIBEAM	30	0x100023f0
NetworkListMACs	31	0x100066d0
PluginDispatch	32	0x100036b0
PluginDispatchEx	33	0x100036e0
PluginDispatchSync	34	0x10003710
PluginDispatchSyncEx	35	0x10003750
PluginGet	36	0x100035a0
PluginOnLoad	37	0x10003650
PluginOnUnload	38	0x10003680
PluginSet	39	0x100035e0
PluginSetEx	40	0x10003610
RegionSave	41	0x10003cd0
RegionScan	42	0x100037b0
RegionScanEx	43	0x10003ac0
SecurityAddDays	44	0x100047c0
SecurityDelete	45	0x10004430
SecurityGetExpiryDate	46	0x100041b0
SecurityGetExpiryFlag	47	0x10004170
SecurityGetTimeNow	48	0x10004270
SecurityGetUserData	49	0x10004210
SecurityIsExpired	50	0x10004290
SecurityIsFirstRun	51	0x10004150
SecurityLoad	52	0x10003e90
SecurityReset	53	0x100046a0
SecuritySave	54	0x10004340
SecuritySetExpiryDate	55	0x100041e0
SecuritySetExpiryFlag	56	0x10004190
SecuritySetUserData	57	0x10004240
SecurityWipeMemory	58	0x10004470
ServerGetPort	73	0x10004d60
ServerGetWindow	74	0x10004d50
ServerIsListening	75	0x10004d70
ServerListen	76	0x10004a80
ServerListenOnPort	77	0x10004b60
ServerSetVirtualRoot	78	0x10004d80
ServerStart	79	0x10004990

Name	Ordinal	Address
ServerStop	80	0x10004cd0
SysInfoGetAdaptersInfo	59	0x10006db0
Test	60	0x10007220
TimeGetFileTime	61	0x10006b40
TimeSync	62	0x10006cc0
ToolsChangeWindowMessageFilter	63	0x10007920
ToolsGetDefaultPrinter	64	0x100077f0
ToolsGetProcessMemoryInfo	65	0x100076f0
ToolsGetStartupWindowState	66	0x100072b0
ToolsIsUserAnAdmin	67	0x100073e0
ToolsLockWorkStation	68	0x10007240
ToolsReleaseMemory	69	0x10007660
ToolsSetDefaultPrinter	70	0x100078c0
ToolsValidateUserCredentials	71	0x100077d0
TransparentAttachChild	81	0x10007db0
TransparentBegin	82	0x10007c50
TransparentBringToFront	83	0x10007e10
TransparentDetachChild	84	0x10007dd0
TransparentEnable	85	0x10007c80
TransparentEnd	86	0x10007e30
TransparentForceMaskedMode	87	0x10007ca0
TransparentFreeze	88	0x10007d40
TransparentIsMaskedMode	89	0x10007cc0
TransparentSetBackgroundColor	90	0x10007d20
TransparentSetChildPos	91	0x10007df0
TransparentSetColorDepth	92	0x10007d00
TransparentSetQuality	93	0x10007ce0
TransparentWMPaint	94	0x10007d60
UtilityIsLoaded	72	0x10002f70

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:27:10.463754892 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:10.523483038 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:12.358792067 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:12.407529116 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:16.026741028 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:16.078315020 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:17.805026054 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:17.856899023 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:18.736902952 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:18.785651922 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:22.220108986 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:22.268802881 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:25.909408092 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:25.969369888 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:27.293838024 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:27.342792034 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:29.895832062 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:29.947455883 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:30.123728037 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:30.172540903 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:39.439891100 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:39.488693953 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:40.642024040 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:40.693648100 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:43.922452927 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:43.971477032 CEST	53	56621	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:27:47.616653919 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:47.675599098 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 15:27:56.377962112 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:27:56.426784039 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:02.646528959 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:02.709189892 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:03.089715958 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:03.094371080 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:03.146033049 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:03.161860943 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:03.456290007 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:03.517818928 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:03.640702963 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:03.697858095 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:04.143016100 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:04.200367928 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:04.627767086 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:04.684884071 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:06.241982937 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:06.303272009 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:06.663604975 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:06.716243029 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:08.210874081 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:08.307351112 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:10.036842108 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:10.131952047 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:10.648545027 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:10.716948986 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:11.577315092 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:11.626153946 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:12.112710953 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:12.169935942 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:12.682240009 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:12.791203976 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:12.877532959 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:12.926136971 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:13.218595028 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:13.275599003 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:13.891577959 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:13.948900938 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:14.660521030 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:14.718916893 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:15.253689051 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:15.302344084 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:15.486116886 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:15.540204048 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:17.129343987 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:17.200845003 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:18.091464043 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:18.143312931 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:18.238210917 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:18.297113895 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:20.888122082 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:20.937088013 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:21.680794954 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:21.742914915 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:25.864119053 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:25.921968937 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:25.971663952 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:25.990525007 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:26.037436962 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:26.070878029 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:26.764676094 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:26.813457966 CEST	53	49944	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:28:44.894730091 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:44.943419933 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:46.601078987 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:46.652355909 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:47.757010937 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:47.805697918 CEST	53	51275	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:48.745296955 CEST	63492	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:48.793936968 CEST	53	63492	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:53.557626009 CEST	58945	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:53.607558012 CEST	53	58945	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:54.168512106 CEST	60779	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:54.218209028 CEST	53	60779	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:54.253176928 CEST	64014	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:54.312875986 CEST	53	64014	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:55.113812923 CEST	57091	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:55.162693024 CEST	53	57091	8.8.8.8	192.168.2.4
Apr 12, 2021 15:28:56.338979959 CEST	55904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:28:56.387799025 CEST	53	55904	8.8.8.8	192.168.2.4

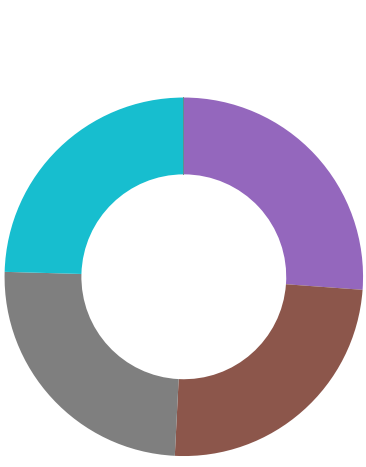
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:28:02.709189892 CEST	8.8.8.8	192.168.2.4	0x4981	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:03.161860943 CEST	8.8.8.8	192.168.2.4	0x3e44	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:03.697858095 CEST	8.8.8.8	192.168.2.4	0x4436	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:04.200367928 CEST	8.8.8.8	192.168.2.4	0x155a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:25.921968937 CEST	8.8.8.8	192.168.2.4	0x88b1	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6788 Parent PID: 6040

General

Start time:	15:27:14
Start date:	12/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\utility.dll'
Imagebase:	0x210000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6836 Parent PID: 6788

General

Start time:	15:27:14
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6868 Parent PID: 6788

General

Start time:	15:27:15
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,CPUSpeed
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6880 Parent PID: 6836

General

Start time:	15:27:15
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 7020 Parent PID: 6880

General

Start time:	15:27:17
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6880 -s 696
Imagebase:	0xbf0000
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	6D161717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC68F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC68F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC68F.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC68F.tmp.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC69D.tmp.csv	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBDF.tmp.txt	success or wait	1	6D154BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 b9 4a 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....Jt`.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.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 3c 1f 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 e0 1a 00 00 b3 4a 74 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 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......<..... ..GenuineIntelW...........T... ....Jt`.................. ....0..1...............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.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 fe ff ff ff 00 00 00 00 00 00 00 00 ec fc 0a 03 6c 00 0a 00 00 00 00 00 24 fd 0a 03 f6 19 00 10 23 00 00 00 46 02 01 00 e0 fc 0a 03 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...+. ..+..................l....... $.......#...F.......+.........	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	168	e4 1a 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 f6 19 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 6c 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 de 24 00 00	....l........... ....$..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	20	0f 00 00 00 e0 e4 43 03 00 00 00 00 04 00 00 00 02 31 00 00	......C..........1..	success or wait	15	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	4	80 f8 29 03	..).	success or wait	14	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	712	bc b1 11 77 d6 c9 0f 77 64 02 00 00 aa aa aa aa 10 00 00 00 cc fd 36 03 98 fe 36 03 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 20 fb 02 00 20 fb 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 20 fb 02 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 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 88 0e 45 03 00 00 00 00 00 00 00 00 38 06 44 03 00 90 fa 02 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 54 92 fa 02 80 f8 29 03 d0 04 44 03 88 f8 29 03 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	...w...wd.............6...6... ..@..w@..w..... ... .d... ....d........ ....E... ......8.D..................... ....T.....)...D...).....................	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.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 aa aa aa aa 00 00 00 00 ec fc 0a 03 aa aa aa aa 00 00 00 00 78 ee 0a 03 bc 9a 11 77 23 00 00 00 06 02 00 00 e8 ec 0a 03 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...+. ..+.......................... x......w#...........+.........	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	48	fc 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 fb 02 00 00 00 00 38 fd 36 03 00 00 00 00 c8 02 00 00 16 84 00 00 cc 02 00 00 42 2d 00 00	....8.6... ....B-..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	50	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	752	00 00 74 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 c4 24 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 dd 02 00 00 00 00 00 20 ef 02 00 00 00 00 ac 4f 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 b6 6d 03 00 00 00 00 00 82 6e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 cb 1a 00 00 00 00 00 37 34 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 0c 39 05 00 00 00 00	..ts.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....`..... ..... .O.....m.....n .....74..... @.....9.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	9958	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...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.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA48.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 1c 15 00 00 9c 07 00 00 05 00 00 00 f4 00 00 00 0e 30 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 b8 1b 00 00 0c 92 00 00 15 00 00 00 ec 01 00 00 b8 1c 00 00 16 00 00 00 98 00 00 00 a4 1e 00 00	....0.....T.....8..... ....T.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.8.0.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 36 00 34 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.>.6.3.6.4.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 33 00 36 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.4.9.3.6.1.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 32 00 38 00 30 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.4.9.2.8.0.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.5.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 38 00 34 00 37 00 38 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.4.7.8.7.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 38 00 34 00 37 00 38 00 37 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.4.7.8.7.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 38 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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.>.1.8.0.3.5.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 37 00 39 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.9.9.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 36 00 32 00 38 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.>.2.6.2.8.0.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 36 00 30 00 30 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.>.2.6.0.0.8.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 32 00 38 00 37 00 39 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.2.8.7.9.3.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 32 00 39 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.2.9.6.1.2.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 32 00 38 00 37 00 39 00 33 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.2.8.7.9.3.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.3.6.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 38 00 39 00 39 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.>.6.8.9.9.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.3.4.4.0.5.1.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 31 00 31 00 31 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.1.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 33 00 37 00 33 00 31 00 34 00 35 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.>.3.7.3.1.4.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 33 00 37 00 31 00 39 00 31 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.9.1.6.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.0.9.6.0.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.5.6.3.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.2.2.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 33 00 34 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.4.8.8.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 33 00 35 00 36 00 37 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.7.6.1.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 33 00 34 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.4.8.8.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.,. .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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 37 00 38 00 30 00 35 00 30 00 36 00 38 00 33 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.>.1.5.7.8.0.5.0.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 31 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.-.0.4.-.1.2.T.1.3.:.2.7.:.2.1.Z.".>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 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 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 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.8.". .P.I.D.=.".6.8.8.0.". .U.p.t.i.m.e.M.S.=.".6.0.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".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.=.".1."	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 64 00 39 00 34 00 62 00 63 00 64 00 38 00 2d 00 37 00 30 00 36 00 65 00 2d 00 34 00 62 00 39 00 31 00 2d 00 39 00 33 00 36 00 30 00 2d 00 64 00 32 00 35 00 36 00 32 00 31 00 31 00 66 00 37 00 35 00 30 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.d.9.4.b.c.d.8.-.7.0.6.e.-.4.b.9.1.-.9.3.6.0.-.d.2.5.6.2.1.1.f.7.5.0.a.<./.G.u.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 31 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.-.0.4.-.1.2.T.1.3.:.2.7.:.2.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC371.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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC68F.tmp.xml	unknown	4623	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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221\Report.wer	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221\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	181	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1b3ef221\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 37 00 39 00 38 00 33 00 37 00 38 00 36 00 34 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.7.9.8.3.7.8.6.4.9.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D1736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D171FB2	RegCreateKeyExW
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D1736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D1736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 F6 19 00 10 02 00 00 00 01 00 00 00 6C 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D171FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 7060 Parent PID: 6868

General

Start time:	15:27:17
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6868 -s 688
Imagebase:	0xbf0000
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	6D161717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC574.tmp.csv	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAB5.tmp.txt	success or wait	1	6D154BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 b9 4a 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....Jt`.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.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 3c 1f 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 d4 1a 00 00 b3 4a 74 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 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......<..... ..GenuineIntelW...........T... ....Jt`.................. ....0..1...............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.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 fe ff ff ff 00 00 00 00 00 00 00 00 44 f7 69 00 68 03 0d 00 00 00 00 00 7c f7 69 00 f6 19 00 10 23 00 00 00 46 02 01 00 38 f7 69 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...+. ..+...............D.i.h....... |.i.....#...F...8.i.+.........	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	168	d8 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 f6 19 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 68 03 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 de 24 00 00	....h........... ....$..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	20	10 00 00 00 3c 9a 11 77 00 00 00 00 00 01 00 00 12 31 00 00	....<..w.........1..	success or wait	16	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	256	c2 08 00 90 b8 54 00 00 00 ba e0 dc 12 77 ff d2 c2 18 00 90 b8 55 00 00 00 ba e0 dc 12 77 ff d2 c2 2c 00 90 b8 56 00 00 00 ba e0 dc 12 77 ff d2 c2 14 00 90 b8 57 00 00 00 ba e0 dc 12 77 ff d2 c2 18 00 90 b8 58 00 00 00 ba e0 dc 12 77 ff d2 c2 0c 00 90 b8 59 00 00 00 ba e0 dc 12 77 ff d2 c2 40 00 90 b8 5a 00 18 00 ba e0 dc 12 77 ff d2 c2 04 00 90 b8 5b 00 1d 00 ba e0 dc 12 77 ff d2 c2 14 00 90 b8 5c 00 00 00 ba e0 dc 12 77 ff d2 c2 10 00 90 b8 5d 00 00 00 ba e0 dc 12 77 ff d2 c2 08 00 90 b8 5e 00 00 00 ba e0 dc 12 77 ff d2 c2 10 00 90 b8 5f 00 00 00 ba e0 dc 12 77 ff d2 c2 14 00 90 b8 60 00 00 00 ba e0 dc 12 77 ff d2 c2 18 00 90 b8 61 00 07 00 ba e0 dc 12 77 ff d2 c2 08 00 90 b8 62 00 00 00 ba e0 dc 12 77 ff d2 c2 1c 00 90 b8 63 00 00 00 ba e0 dc 12 77 ff	.....T.......w.......U.......w ...,...V.......w.......W...... .w.......X.......w.......Y.... ...w...@...Z.......w.......[.. .....w.......\.......w.......] ....w.......^.......w...... ._.......w.......`.......w.... ...a.......w.......b.......w.. .....c.......w.	success or wait	15	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	1468	bc b1 11 77 d6 c9 0f 77 60 02 00 00 aa aa aa aa 10 00 00 00 d8 fa 25 04 a4 fb 25 04 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 40 52 00 00 40 52 00 00 00 00 00 60 02 00 00 aa aa aa aa 60 02 00 00 aa aa aa aa 00 40 52 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 00 aa aa aa aa d0 05 87 00 00 00 00 00 00 00 00 00 40 07 86 00 00 b0 51 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 54 b2 51 00 9c f8 a0 02 d8 05 86 00 a4 f8 a0 02 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.....@R..@R..... `.......`........@R.............. ....@.....Q................ ........................T.Q...	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.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 aa aa aa aa 00 00 00 00 44 f7 69 00 aa aa aa aa 00 00 00 00 d0 e8 69 00 bc 9a 11 77 23 00 00 00 12 02 00 00 40 e7 69 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...+. ..+...............D.i......... ..i....w#.......@.i.+.........	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	48	ec 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 40 52 00 00 00 00 00 44 fa 25 04 00 00 00 00 bc 05 00 00 b6 89 00 00 cc 02 00 00 42 2d 00 00	....@R.....D.%... ....B-..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	50	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	752	00 00 74 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 c4 24 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 23 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 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 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 d0 da 02 00 00 00 00 00 20 ef 02 00 00 00 00 63 4f 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 58 6e 03 00 00 00 00 00 7c 6e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a ca 1a 00 00 00 00 00 26 35 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 0c 39 05 00 00 00 00	..ts.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... .... cO.....Xn.....|n .....&5..... @.....9.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	9850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA0A.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 1c 15 00 00 9c 07 00 00 05 00 00 00 04 01 00 00 0e 30 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 68 1b 00 00 84 9a 00 00 15 00 00 00 ec 01 00 00 b8 1c 00 00 16 00 00 00 98 00 00 00 a4 1e 00 00	....0.....T.....8..... ....T.....h.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.6.8.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 34 00 33 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.>.6.1.4.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 33 00 36 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.4.9.3.6.1.9.2.<./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 39 00 32 00 38 00 30 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.4.9.2.8.0.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 35 00 31 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.5.1.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 38 00 35 00 31 00 35 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.5.1.5.5.8.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 38 00 35 00 31 00 35 00 35 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.>.8.5.1.5.5.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 38 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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.>.1.8.0.3.5.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 37 00 39 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.9.9.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 36 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.>.2.6.3.4.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 36 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.>.2.6.0.7.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 35 00 33 00 30 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.3.0.4.3.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 35 00 33 00 31 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.3.1.2.5.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 35 00 33 00 30 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.3.0.4.3.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.7.8.8.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 33 00 33 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.>.6.9.3.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 31 00 37 00 31 00 30 00 38 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.7.1.0.8.9.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 31 00 33 00 30 00 37 00 38 00 35 00 32 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.>.1.3.0.7.8.5.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	72	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 39 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.0.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.4.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 33 00 30 00 36 00 37 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.>.3.0.6.7.9.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.5.2.8.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.6.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 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.>.5.2.2.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.1.3.6.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.5.3.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.,. .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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 37 00 38 00 30 00 35 00 30 00 36 00 38 00 33 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.>.1.5.7.8.0.5.0.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 31 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.-.0.4.-.1.2.T.1.3.:.2.7.:.2.1.Z.".>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 39 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 39 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.7.". .P.I.D.=.".6.8.6.8.". .U.p.t.i.m.e.M.S.=.".3.9.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.9.0.". .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.=.".1."	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 63 00 34 00 38 00 37 00 33 00 36 00 36 00 2d 00 66 00 63 00 38 00 61 00 2d 00 34 00 66 00 61 00 65 00 2d 00 62 00 39 00 37 00 36 00 2d 00 31 00 66 00 33 00 35 00 34 00 36 00 66 00 34 00 39 00 66 00 33 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.c.4.8.7.3.6.6.-.f.c.8.a.-.4.f.a.e.-.b.9.7.6.-.1.f.3.5.4.6.f.4.9.f.3.e.<./.G.u.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 31 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.-.0.4.-.1.2.T.1.3.:.2.7.:.2.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC277.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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC566.tmp.xml	unknown	4623	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 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465\Report.wer	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465\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	180	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_1bc6e465\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 31 00 31 00 30 00 39 00 39 00 38 00 37 00 36 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.1.1.0.9.9.8.7.6.9.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1543D1	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

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	05 00 00 C0 00 00 00 00 00 00 00 00 F6 19 00 10 02 00 00 00 01 00 00 00 6C 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 F6 19 00 10 02 00 00 00 01 00 00 00 68 03 0D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D171FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 7124 Parent PID: 6788

General

Start time:	15:27:18
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6080 Parent PID: 7124

General

Start time:	15:27:20
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 688
Imagebase:	0xbf0000
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	6D161717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA46.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA46.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_17936916	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_17936916\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA46.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA46.tmp.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA86.tmp.csv	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF0B.tmp.txt	success or wait	1	6D154BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 bd 4a 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....Jt`.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.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 3c 1f 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 d4 1b 00 00 b6 4a 74 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 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......<..... ..GenuineIntelW...........T... ....Jt`.................. ....0..1...............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.............. ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.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 00 40 9c 00 00 00 00 00 26 9f 71 01 80 9f 71 01 3c ed 95 00 3c ed 95 00 20 d0 97 04 5f f1 00 10 23 00 00 00 46 02 01 00 0c ed 95 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 aa aa aa aa aa aa	....+...S...+. ..+....@......&.q...q..<...<... ..._...#...F.......+.........	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	168	d8 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 5f f1 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 9c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 de 24 00 00	......................_..... ....@.......... ....$..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	20	12 00 00 00 00 90 b1 02 00 00 00 00 98 04 00 00 32 31 00 00	................21..	success or wait	18	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 9b 00 a0 7b 1c 77 38 17 e2 02 00 00 00 00 00 00 e2 02 a0 79 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 5c 74 00 00 00 00 00 00 00 00 00 00 8c 00 00 00 00 00 f8 7b 1c 77 ff ff ff ff 07 00 00 00 00 00 6d 7f 00 00 00 00 30 07 6d 7f 00 00 7d 7f 28 02 7e 7f 50 06 7f 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 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 1c 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 0a 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	.............{.w8............y .w..............\t................. {.w..........m.....0.m...}. (.~.P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	17	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	4	74 68 65 6d	them	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.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 aa aa aa aa 00 00 00 00 aa aa aa aa 3c ed 95 00 00 00 00 00 a0 de 95 00 bc 9a 11 77 23 00 00 00 12 02 00 00 10 dd 95 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...+. ..+..................<....... ....w#...........+........	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	48	e4 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 b2 02 00 00 00 00 00 98 f7 6f 04 00 00 00 00 68 08 00 00 b6 91 00 00 cc 02 00 00 42 2d 00 00	....o... ..h...........B-..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	50	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	752	00 00 74 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 c4 24 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 c0 c8 02 00 00 00 00 00 20 ef 02 00 00 00 00 78 55 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 2b 6d 03 00 00 00 00 00 eb 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 87 1a 00 00 00 00 00 88 77 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 1d 7e 05 00 00 00 00	..ts.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... .... xU.....+m.....p .....w..... @.....~.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	9850	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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC65E.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 1c 15 00 00 9c 07 00 00 05 00 00 00 24 01 00 00 0e 30 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 68 1b 00 00 50 a6 00 00 15 00 00 00 ec 01 00 00 b8 1c 00 00 16 00 00 00 98 00 00 00 a4 1e 00 00	.....$. ...0.....T.....8..... ....T.....h...P.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.2.4.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 36 00 33 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.>.7.6.3.8.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 39 00 32 00 31 00 37 00 32 00 38 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.>.1.4.9.2.1.7.2.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 39 00 32 00 30 00 39 00 30 00 38 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.>.1.4.9.2.0.9.0.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 38 00 34 00 33 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.8.4.3.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 37 00 31 00 30 00 36 00 35 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.>.3.2.7.1.0.6.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 33 00 32 00 37 00 31 00 30 00 36 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.2.7.1.0.6.5.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 38 00 30 00 31 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.0.1.2.8.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 37 00 39 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.9.9.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.2.1.5.9.8.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 37 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.5.7.1.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 39 00 35 00 35 00 32 00 36 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.5.5.2.6.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 32 00 39 00 35 00 36 00 30 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.5.6.0.8.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 39 00 35 00 35 00 32 00 36 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.5.5.2.6.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.7.8.8.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 36 00 38 00 33 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.>.1.1.6.8.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 31 00 37 00 31 00 30 00 38 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.7.1.0.8.9.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 31 00 33 00 30 00 37 00 38 00 35 00 32 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.>.1.3.0.7.8.5.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	72	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 39 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.6.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.4.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 33 00 30 00 36 00 37 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.>.3.0.6.7.9.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.5.2.8.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.6.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 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.>.5.2.2.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.1.3.6.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.F.i.l.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.a.g.e.F.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.F.i.l.e.U.s.a.g.e.>.6.5.5.3.6.0.<./.P.e.a.k.P.a.g.e.F.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.,. .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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 37 00 38 00 30 00 35 00 30 00 36 00 38 00 33 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.>.1.5.7.8.0.5.0.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 36 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.-.0.4.-.1.2.T.1.3.:.2.7.:.2.6.Z.".>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 38 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.7.". .P.I.D.=.".7.1.2.4.". .U.p.t.i.m.e.M.S.=.".4.8.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.8.4.". .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.=.".1."	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 32 00 62 00 38 00 39 00 62 00 33 00 65 00 2d 00 35 00 31 00 64 00 65 00 2d 00 34 00 61 00 65 00 34 00 2d 00 61 00 34 00 63 00 30 00 2d 00 32 00 66 00 61 00 39 00 35 00 36 00 66 00 32 00 66 00 64 00 33 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.2.b.8.9.b.3.e.-.5.1.d.e.-.4.a.e.4.-.a.4.c.0.-.2.f.a.9.5.6.f.2.f.d.3.4.<./.G.u.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 32 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.1.2.T.1.3.:.2.7.:.2.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD4A7.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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA46.tmp.xml	unknown	4623	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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f892833bb6a965bb21678f4e1a_82810a17_17936916\Report.wer	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f892833bb6a965bb21678f4e1a_82810a17_17936916\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	181	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f892833bb6a965bb21678f4e1a_82810a17_17936916\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 31 00 39 00 38 00 30 00 32 00 34 00 31 00 32 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.1.9.8.0.2.4.1.2.6.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1543D1	unknown

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	05 00 00 C0 00 00 00 00 00 00 00 00 F6 19 00 10 02 00 00 00 01 00 00 00 68 03 0D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 5F F1 00 10 02 00 00 00 00 00 00 00 00 40 9C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D171FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 3492 Parent PID: 6788

General

Start time:	15:27:21
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt2BinStr
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 4544 Parent PID: 3492

General

Start time:	15:27:23
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3492 -s 688
Imagebase:	0xbf0000
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	6D161717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_11932288	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_11932288\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D15497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp.xml	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA36.tmp.csv	success or wait	1	6D154BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFE4.tmp.txt	success or wait	1	6D154BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 c5 4a 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....Jt`.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.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 3c 1f 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 a4 0d 00 00 b9 4a 74 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 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00	.....U.....B.....<..... ..GenuineIntelW.....T... .....Jt`..... .....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.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 00 40 9c 00 00 00 00 00 95 1a 7e 01 80 70 af 04 7c eb b7 02 7c eb b7 02 20 70 af 04 5f f1 00 10 23 00 00 00 46 02 01 00 4c eb b7 02 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...+. ..+....@........~..p..|...|... p.._...#...F...L...+.........	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	168	68 16 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 5f f1 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 9c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 de 24 00 00	h......................._..... ....@.......... ....$..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	20	12 00 00 00 00 20 d1 02 00 00 00 00 98 04 00 00 32 31 00 00	....21..	success or wait	18	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 9b 00 a0 7b 1c 77 38 17 fb 02 00 00 00 00 00 00 fb 02 a0 79 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 5c 74 00 00 00 00 00 00 00 00 00 00 ae 02 00 00 00 00 f8 7b 1c 77 ff ff ff ff 07 00 00 00 00 00 50 7f 00 00 00 00 30 07 50 7f 00 00 60 7f 28 02 61 7f 50 06 62 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 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 1c 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 0a 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	............{.w8...........y .w.............\t................ {.w..........P.....0.P...`. (.a.P.b................m........ ..................`f.w.. ....PS.w.........B......	success or wait	17	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	2004	bc b1 11 77 d6 c9 0f 77 5c 02 00 00 aa aa aa aa 10 00 00 00 c0 f8 8f 04 8c f9 8f 04 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 b0 d1 02 00 b0 d1 02 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 b0 d1 02 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 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 07 fd 02 00 00 00 00 00 00 00 00 50 07 fc 02 00 20 d1 02 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 54 22 d1 02 98 fc f7 02 e8 05 fc 02 a0 fc f7 02 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................\... ....\........................ ....P.... ....T"....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.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 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa 7c eb b7 02 00 00 00 00 e0 dc b7 02 bc 9a 11 77 23 00 00 00 16 02 00 00 50 db b7 02 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 aa aa aa aa aa aa	?............................ ....+...S...+. ..+..................|....... ....w#.......P...+.........	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	48	e0 07 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 b0 d1 02 00 00 00 00 2c f8 8f 04 00 00 00 00 00 d4 07 00 00 d2 91 00 00 cc 02 00 00 42 2d 00 00	....,..... ....B-..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	50	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	752	00 00 74 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 c4 24 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 ac 02 00 00 00 00 00 20 ef 02 00 00 00 00 3d 5a 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 b3 73 03 00 00 00 00 00 cf 74 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e5 85 1a 00 00 00 00 00 5b 79 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 58 a5 05 00 00 00 00	..ts.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....@..... ..... =Z.....s.....t .....[y..... @.....X.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	9850	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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD94A.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 1c 15 00 00 9c 07 00 00 05 00 00 00 24 01 00 00 0e 30 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 68 1b 00 00 b8 a4 00 00 15 00 00 00 ec 01 00 00 b8 1c 00 00 16 00 00 00 98 00 00 00 a4 1e 00 00	..... $. ...0.....T.....8..... ....T.....h.....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.9.2.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 30 00 37 00 36 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.>.1.2.0.7.6.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 30 00 30 00 31 00 31 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.5.0.0.1.1.9.0.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 30 00 30 00 30 00 33 00 37 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.5.0.0.0.3.7.1.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 38 00 36 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.8.6.3.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 33 00 35 00 32 00 39 00 38 00 35 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.>.3.3.5.2.9.8.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 33 00 33 00 35 00 32 00 39 00 38 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.3.5.2.9.8.5.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 38 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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.>.1.8.0.3.5.2.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 38 00 30 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.0.1.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 32 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.2.2.2.4.1.6.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 32 00 31 00 34 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.>.2.2.2.1.4.4.<./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 30 00 33 00 38 00 30 00 30 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.3.8.0.0.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 30 00 33 00 38 00 38 00 32 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.3.8.8.2.2.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 30 00 33 00 38 00 30 00 30 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.3.8.0.0.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.7.8.8.<./.P.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 33 00 38 00 36 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.>.1.9.3.8.6.<./.U.p.t.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 31 00 37 00 31 00 30 00 38 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.7.1.0.8.9.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 31 00 33 00 30 00 37 00 38 00 35 00 32 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.>.1.3.0.7.8.5.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 31 00 30 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.0.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.4.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 33 00 30 00 36 00 37 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.>.3.0.6.7.9.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 00 61 00 67 00 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.>.3.2.5.2.8. <./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.6.5.6. <./.Q.u. o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 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.>.5.2.2.4. <./.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.1.3.6. <./. 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.5.3.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.,. .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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 79 00 74 00 62 00 71 00 77 00 77 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.>.y.t.b.q.w.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 37 00 38 00 30 00 35 00 30 00 36 00 38 00 33 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.>.1.5.7.8.0.5.0.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 33 00 34 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.-.0.4.-.1.2.T.1.3.:.2.7.:.3.4.Z.".>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 33 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.7.1.". .P.I.D.=.".3.4.9.2.". .U.p.t.i.m.e.M.S.=.".5.3.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".5.3.1.". .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.=.".1."	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 64 00 30 00 37 00 31 00 36 00 63 00 33 00 2d 00 36 00 62 00 36 00 36 00 2d 00 34 00 63 00 37 00 63 00 2d 00 62 00 33 00 31 00 63 00 2d 00 38 00 35 00 61 00 30 00 35 00 38 00 32 00 66 00 32 00 33 00 66 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.d.0.7.1.6.c.3.-.6.b.6.6.-.4.c.7.c.-.b.3.1.c.-.8.5.a.0.5.8.2.f.2.3.f.2.<./.G.u.i.d.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 32 00 37 00 3a 00 33 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.1.2.T.1.3.:.2.7.:.3.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2DE.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	6D15497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF957.tmp.xml	unknown	4623	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	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_11932288\Report.wer	unknown	2	ff fe	..	success or wait	1	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_11932288\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	181	6D15497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_11932288\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 31 00 31 00 36 00 30 00 32 00 33 00 31 00 30 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.1.1.6.0.2.3.1.0.4.	success or wait	1	6D15497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1736BF	unknown
\REGISTRY\A\{19f58abe-5348-b73a-d421-f3e486298b5e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1543D1	unknown

Analysis Process: rundll32.exe PID: 4264 Parent PID: 6788

General

Start time:	15:27:25
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DecryptEx

Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6384 Parent PID: 6788

General

Start time:	15:27:28
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,Deflate
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6528 Parent PID: 6788

General

Start time:	15:27:32
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DeflateToMemory
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6656 Parent PID: 6788

General

Start time:	15:27:35
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawEnumDisplayModes
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6136 Parent PID: 6788

General

Start time:	15:27:39
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawIsSupported
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6308 Parent PID: 6788

General

Start time:	15:27:42
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawRestoreDisplayMode
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4108 Parent PID: 6788

General

Start time:	15:27:45
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawSetDisplayMode
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6096 Parent PID: 6788

General

Start time:	15:27:49
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryAdd
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 4612 Parent PID: 6096

General

Start time:	15:27:51
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6096 -s 688
Imagebase:	0xbf0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6672 Parent PID: 6788

General

Start time:	15:27:53
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryClear
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7064 Parent PID: 6788

General

Start time:	15:27:56
Start date:	12/04/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryDump
Imagebase:	0x9b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis