ID: 385485
Sample Name: utility.dll
Cookbook: default.jbs
Time: 15:36:36
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

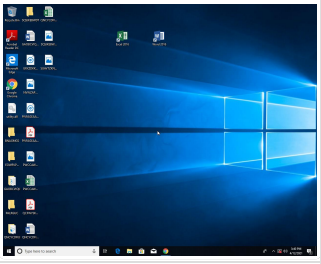
Analysis Report utility.dll

Overview

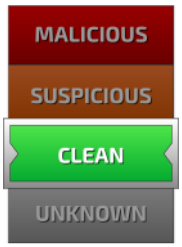
General Information

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

Most interesting Screenshot:



Detection

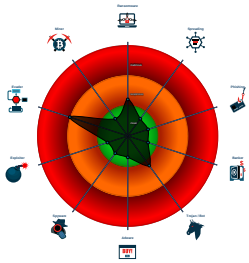


Score:	8
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

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



Analysis Advice

Sample crashes during execution, try analyze it on another analysis machine

Sample may be VM or Sandbox-aware, try analysis on a native machine

Startup

- **System is w10x64**
- loaddll32.exe (PID: 3664 cmdline: loaddll32.exe 'C:\Users\user\Desktop\utility.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4080 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 908 cmdline: rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1956 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 908 -s 696 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 460 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,CPUSpeed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5360 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 460 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4120 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5816 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4120 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5436 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Decrypt2BinStr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5512 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5436 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5988 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DecryptEx MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5352 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5988 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4928 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,Deflate MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3580 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4928 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1268 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DeflateToMemory MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3512 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1268 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 3352 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawEnumDisplayModes MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5716 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawIsSupported MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5324 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawRestoreDisplayMode MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3544 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectDrawSetDisplayMode MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6220 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryAdd MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6332 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6220 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6356 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryClear MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6444 cmdline: rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryDump MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

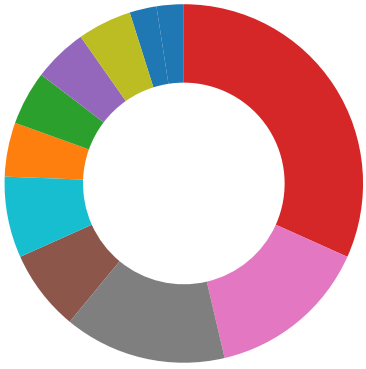
Yara Overview

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

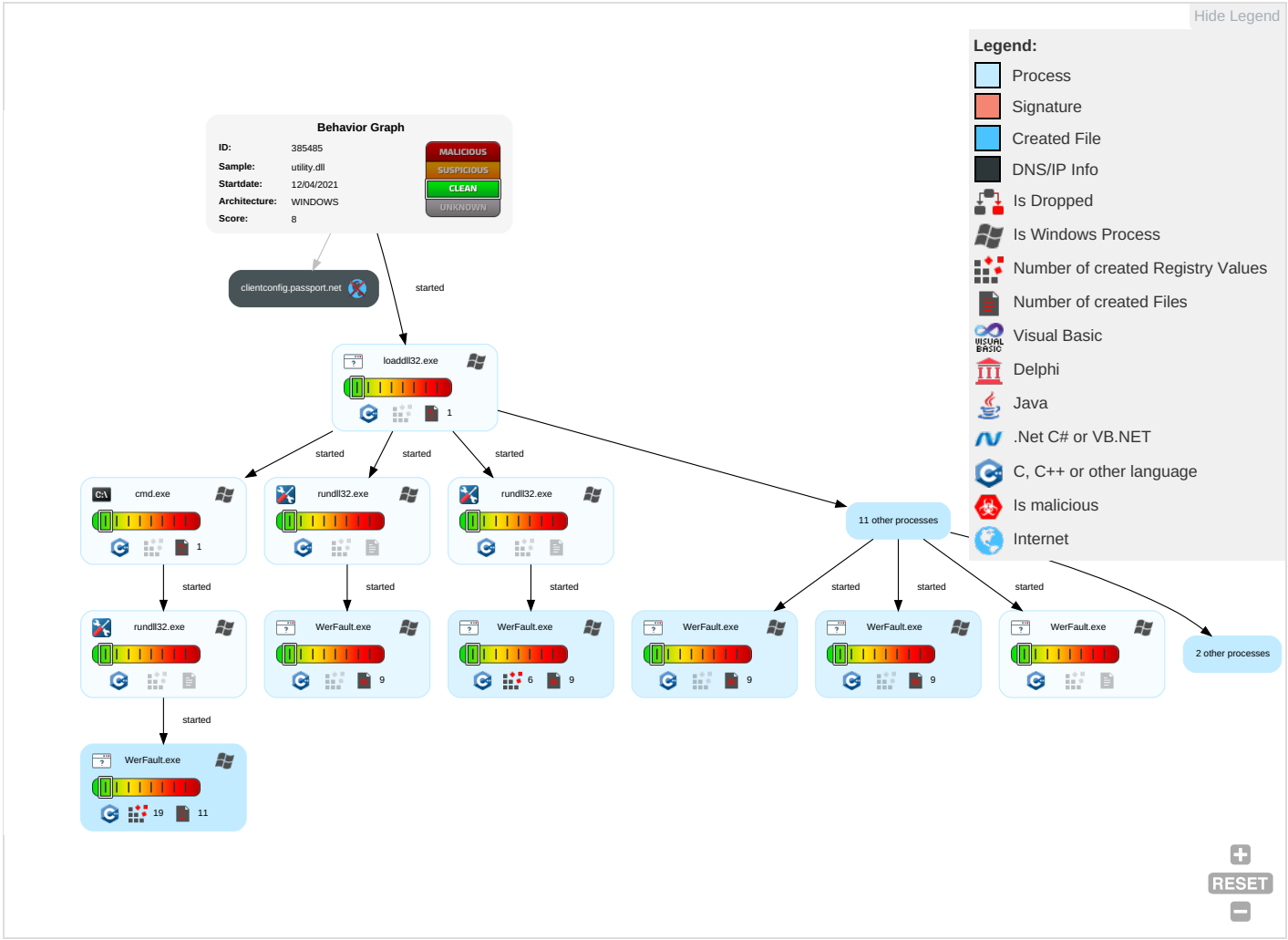
There are no malicious signatures, click here to show all signatures.

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 2	Virtualization/Sandbox Evasion 1 2	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 Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	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	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Virtualization/Sandbox Evasion 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

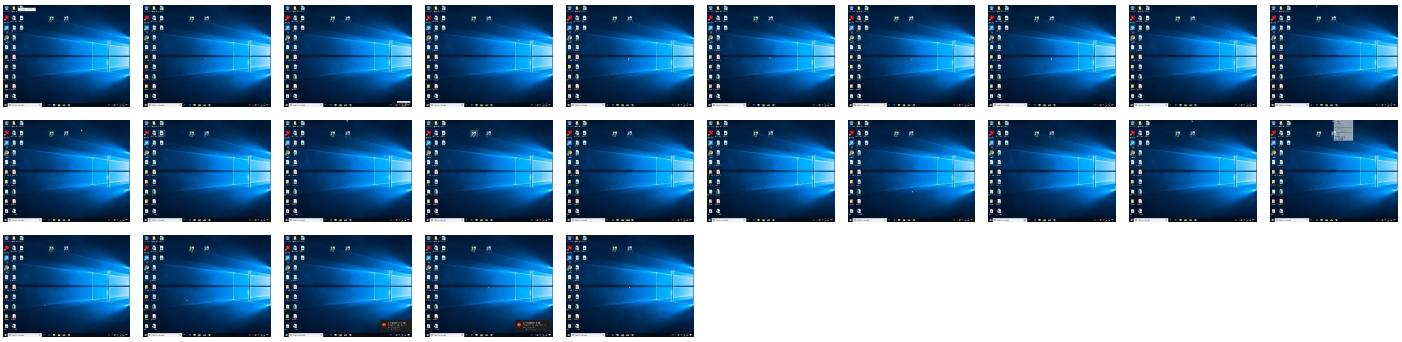
Behavior Graph



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

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.thawte.com/repository0	utility.dll	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	utility.dll	false		high
http://https://www.thawte.com/cps0/	utility.dll	false		high
http://ocsp.thawte.com0	utility.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: 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:	15:36:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
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
Run name:	Run with higher sleep bypass
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@51/32@1/0
EGA Information:	• Successful, ratio: 60%
HDC Information:	• Successful, ratio: 100% (good quality ratio 96%) • Quality average: 85% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 168.61.161.212, 20.190.160.135, 20.190.160.3, 20.190.160.5, 20.190.160.72, 20.190.160.130, 20.190.160.70, 20.190.160.9, 20.190.160.7, 40.126.31.142, 40.126.31.3, 20.190.159.131, 40.126.31.136, 40.126.31.7, 40.126.31.138, 20.190.159.133, 40.126.31.140, 40.126.31.141, 40.126.31.137, 20.190.159.132, 40.126.31.4, 20.190.159.138, 20.190.159.134, 40.126.31.6, 40.126.31.135, 20.50.102.62, 13.64.90.137, 184.30.24.56, 92.122.213.194, 92.122.213.247, 88.221.62.148, 92.123.150.225, 20.54.26.129, 20.82.210.154, 104.43.193.48, 20.82.209.183, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.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, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, login.live.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Execution Graph export aborted for target rundll32.exe, PID 1268 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 4928 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

No simulations

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_07c90a00\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12316
Entropy (8bit):	3.7670478879483698
Encrypted:	false
SSDEEP:	192:zyi60oXHR+HBUZMX4jed+h+/u7sHS274ItWc4:eisXwBUZMX4jes+/u7sHX4ItWc4
MD5:	3739D5CB15C54D39E0AD41B058ACEFBB
SHA1:	3C8AA7B070843389630656CEB320FD0E33126BB4
SHA-256:	DABE06FEF7238F688E262C2AD6F0091A8A251A8772E0C5BBB793DD0F533216F3
SHA-512:	EC3D02A8ABCACDE4DE77C8A4116534DDFBCB655CFBC9C0BBF686E02DBA9B5C64B36EE081F4AFBECC525F4A2DF1FE1AD60FB7858DE32A5427808DD2A426A 2626
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.=.1.3.2.6.2.7.4.0.6.4.2.9.4.2.7.0.2.1.....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.=.1.3.2.6.2.7.4.0.6.4.3.8.4.8.9.5.0.7.....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.=.b.d.0.c.a.2.a.5.-.7.f.e.b.-.4.4.5.1.-.a.b.a.f.-.5.6.b.b.7.3.1.d.3.6.d.6.....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.=.1.7.1.5.c.2.9.0.-.d.9.a.2.-.4.1.7.a.-.a.0.e.d.-.c.7.9.8.2.6.6.3.b.9.3.9.....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.=.0.0.0.0.0.3.8.c.-.0.0.0.1.-.0.0.1.7.-.3.0.6.c.-.8.d.6.6.e.c.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_149cdf75\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12316
Entropy (8bit):	3.7661877574680434
Encrypted:	false
SSDEEP:	192:hw2i/0oXfR+HBUZMX4jed+h+/u7sHS274ItWck:G2iBXIBUZMX4jes+/u7sHX4ItWck
MD5:	B3E686E1B3CD967341B02DCF749ACE32
SHA1:	3EE9654A866AC0AE1E2DF834EC0F925EDE86F2CC
SHA-256:	CE2FDD0FC85642F82D811D320D5000A978A17E4A2C8AD7124AA6F1C9E52BAD6E
SHA-512:	BBCD1EBFB1E2C79352C268246E1DA7363721DD5F0885A720BF44371183B7D7BAB6245DFA8E8A7DA013B35D9F7DD8AF7BECAD152AEB703123C4F088B5658FA9 CB
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.=.1.3.2.6.2.7.4.0.6.4.2.8.4.8.9.5.3.5.....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.=.1.3.2.6.2.7.4.0.6.4.3.6.9.2.7.0.2.8.....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.=.8.4.0.5.a.2.2.1.-.3.a.3.3.-.4.8.6.8.-.9.e.5.0.-.b.e.8.e.a.6.3.0.b.0.e.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.=.4.1.2.0.9.c.6.d.-.2.a.5.4.-.4.7.2.0.-.a.f.4.a.-.5.3.5.c.b.5.c.a.b.e.e.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.=.0.0.0.0.0.1.c.c.-.0.0.0.1.-.0.0.1.7.-.2.3.0.f.-.8.a.6.6.e.c.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_35213f9598763c4410dce51d5b87d739df16f5ab_82810a17_0dd51c5f\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):	3.766832839700023
Encrypted:	false
SSDEEP:	192:jIie0oXgFHBUZMX4jed+h+/u7sHS274ItWcB:cioXwBUZMX4jec+/u7sHX4ItWcB
MD5:	427FAB10FF298CDCE88B1F3AEDA166FA
SHA1:	C23339EE9E8781488D2B2D348561A5AB9B973208
SHA-256:	BA0B85C367E5D2355C284069675EACBBCBDBBC9C70E7E382AFD2766B6C34F4CC
SHA-512:	5AC9C7ED476E191CA3C635C3B1A5E817B1ED6A442D7EC76FBECD7CF35F90713510C92CB83707D1E411E4CE9011317EEA6166A5918AB02C2C12A87F9E89A81A6
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.=.1.3.2.6.2.7.4.0.6.5.9.2.0.8.2.8.8.8.....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.=.1.3.2.6.2.7.4.0.6.5.9.8.9.5.7.8.9.7.....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.=.9.4.7.8.4.2.e.7.-.a.8.0.c.-.4.e.a.6.-.8.c.3.3.-.7.e.a.1.8.a.1.b.4.b.6.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.5.0.6.d.2.0.5.-.d.7.d.0.-.4.7.4.8.-.8.1.2.c.-.d.6.5.3.5.e.a.2.c.8.e.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.=.0.0.0.0.0.4.f.4.-.0.0.0.1.-.0.0.1.7.-.c.d.5.d.-.6.7.7.0.e.c.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_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146\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):	3.7680524054368094
Encrypted:	false
SSDEEP:	192:OuNnciav0oXfEHBUZMX4jed+h+/u7sHS274ItWcI:TciaRXkBUZMX4jec+/u7sHX4ItWcI
MD5:	E2714D71D6DCA8722CCBC2EB084DAFD2
SHA1:	73B10EAE55074EF6CB8EFBDBBA451B54E3544AEA
SHA-256:	F00DA5A6E67E3AECCF0F80A8C11C18BF43552FC0FF6AF65B3DF2A5257357A21D
SHA-512:	C8D3F4F903BEA8002E700B2BC974E349B755DA95F803FEAD4565EDD21F5B168DE7977470066F497B3445494617F8401713C6D169D6B46F21DA517A49805D6A2E
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.=.1.3.2.6.2.7.4.0.6.5.2.2.0.8.3.0.7.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.7.4.0.6.5.2.9.5.8.3.0.3.9.....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.=.e.5.9.8.3.1.f.5.-.a.1.e.d.-.4.2.1.6.-.b.9.8.6.-.7.3.3.6.c.7.0.e.b.9.f.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.5.3.8.8.8.d.3.-.4.9.3.9.-.4.c.5.7.-.a.a.4.f.-.6.f.0.3.9.6.e.3.f.6.a.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.6.4.-.0.0.0.1.-.0.0.1.7.-.1.8.a.2.-.5.d.6.c.e.c.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_692d4c8e33a25a7b2ade9d9882c855426fd2f6ba_82810a17_0d911579\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12294
Entropy (8bit):	3.7685429762791665
Encrypted:	false
SSDEEP:	192:EbSiJ0oXJKVHBUZMX4jed+h+/u7sHS274ItWcA:pinXgFBUZMX4jec+/u7sHX4ItWcA
MD5:	054AC5266528EDFAC39D109AB01E5E9F
SHA1:	0F5C9DB4374B023302C1E5053BE4A5955C940CDB
SHA-256:	621046744C822A4966A1ED5ED8351CDC35375329BE8BCA086CA7BB91E3AD7DE7
SHA-512:	8B9113A5F3A376A3394869DC385B0E127EE092EA6F5E7B1A405954A7C7210BEDB60AC928723BF067CF2F6261CBED0251991EFA2654B5A9B323BF1B5DA9A212A
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.=.1.3.2.6.2.7.4.0.6.5.6.0.3.6.4.2.2.3.....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.=.1.3.2.6.2.7.4.0.6.5.8.1.3.0.1.6.8.1.....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.=.5.b.d.9.7.5.9.8.-.4.d.9.1.-.4.7.5.6.-.8.5.1.4.-.6.5.1.f.6.a.0.b.6.f.1.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.0.8.f.4.a.3.e.-.c.7.6.0.-.4.8.6.f.-.a.1.a.7.-.2.b.4.7.0.a.3.1.1.b.8.3.....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.=.0.0.0.0.1.3.4.0.-.0.0.0.1.-.0.0.1.7.-.f.f.6.b.-.4.d.6.e.e.c.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_18d1d4b3\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6995fa83d7b0318a43db0d33e1e8ff1c3499353_82810a17_18d1d4b3\Report.wer	
Category:	dropped
Size (bytes):	12320
Entropy (8bit):	3.768720719394826
Encrypted:	false
SSDEEP:	192:mvf0cFiV0oXtHBUZMX4jed+h+/u7ssS274ItWcM:Wfi7X9BUZMX4jec+/u7ssX4ItWcM
MD5:	088490B0E004EAA681E41123663AEA8B
SHA1:	87811A313B8F043B488DAAD633DE46F83D9F10C0
SHA-256:	DE86A9A13F287A733F04A6861000A9CE7D104FC43914967285819CFCBB4BBBF1
SHA-512:	3C856150E5C1FAF8294A7CE0D4414691A34FD7210FA4F8F285BAD6DF8CF60CDAA44BB50BB1C95A6F80894F79D2C7976EB1F3BE321D2D6A55FC3775A647A8CBC
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.=.1.3.2.6.2.7.4.0.6.7.6.4.8.9.4.9.9.2.....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.=.1.3.2.6.2.7.4.0.6.7.7.8.8.0.1.2.4.5.....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.=.6.b.8.3.2.b.9.7.-.2.a.6.d.-.4.0.a.1.-.b.a.2.b.-.5.5.2.b.9.b.0.d.f.c.2.d.....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.=.8.7.9.9.d.0.b.7.-.d.a.5.a.-.4.f.2.a.-.9.4.5.c.-.5.0.6.b.5.8.3.e.7.c.e.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.8.4.c.-.0.0.0.1.-.0.0.1.7.-.d.4.5.b.-.2.8.7.a.e.c.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_15e4f4b3\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):	3.76863374951274
Encrypted:	false
SSDEEP:	192:OliK0oXxqHBUZMX4jed+h+/u7sHS274ItWc4:oicX0BUZMX4jes+/u7sHX4ItWc4
MD5:	FE4A03FCD8B5859A9DF5544296AC6014
SHA1:	0126539A895BED1A6B483CE58A9AD30E3BD70968
SHA-256:	451144CC6B63C47909D2742BD056695574C2AC899FEA1E37318D4F7DC845533D
SHA-512:	6199F8CFD1191E623117464FE02A92752BE5CBBDB4FF20E8596923733AC6D3160202736AFEA5D12FC44DC0475A21782A9E21E075E12CA54DAD6ABB737233BAD
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.=.1.3.2.6.2.7.4.0.6.4.9.0.5.2.0.6.7.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.7.4.0.6.4.9.7.3.9.5.6.2.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.6.1.e.3.d.f.-.9.7.0.7.-.4.c.8.6.-.9.5.0.7.-.4.b.1.d.6.8.7.4.1.b.4.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.a.e.3.e.3.9.2.-.f.8.8.4.-.4.7.8.a.-.8.3.f.1.-.9.3.8.c.7.e.e.6.9.a.3.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.5.3.c.-.0.0.0.1.-.0.0.1.7.-.0.f.3.8.-.6.b.6.a.e.c.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_16d4e8ad\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12314
Entropy (8bit):	3.7695893550245785
Encrypted:	false
SSDEEP:	192:qDGi20oX0qHBUZMX4jed+B+/u7sHS274ItWck:GGiwXRBUZMX4jeM+/u7sHX4ItWck
MD5:	0EE5A43B8A1EA3C7F44B770AD845375D
SHA1:	55BBF243D86AE27553B87811868496151B592D62
SHA-256:	2C47A4C5A50F2FDB29412A52A25132BBBDDC055162FFC1283E818BF39F12F57D
SHA-512:	54AF33487705E7E88B09449CA3122470FF72AACA3C975A023625078DA0B9A8067F11EDE6855FCA888AEF5C7CAF1359AB97A08EF94FA55545D283484B86D7A2DD
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.=.1.3.2.6.2.7.4.0.6.4.5.8.1.7.7.0.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.7.4.0.6.4.6.6.6.1.4.4.5.5.....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.=.d.5.f.1.a.0.8.8.-.9.e.5.0.-.4.7.1.2.-.b.0.7.3.-.a.4.3.f.3.c.f.b.6.4.d.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.b.9.9.f.8.7.5.-.9.5.3.4.-.4.0.0.6.-.a.f.8.d.-.d.b.8.8.c.3.3.c.2.9.4.d.....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.=.0.0.0.0.1.0.1.8.-.0.0.0.1.-.0.0.1.7.-.f.e.2.4.-.7.b.6.8.e.c.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\WER106A.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):	3.694052520088763

C:\ProgramData\Microsoft\Windows\WER\Temp\WER106A.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiSY6H6YlH6ag5BgmfTk3SYaCpr989b8hsfsUm:RrlsNiN6H6Y16aIgmfTk3SY48afW
MD5:	2824E6215E50A019396614F4032D5B17
SHA1:	701A66B90FC0BDDDC45FE30C7F830714D9C4221B
SHA-256:	0DB773CB57811D90FD5F47501B44D9084DC692D9A9CE4E4FDCEC60508919C4A1
SHA-512:	FB9A549427E90351D3122D827FB1EF00A7147C46E639D445D596043928993B1A38C711392E61BACF6F315AC14AA7B09BCAF5FBA9FD643C88DF5D08CE2C96BD4
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.>.4.9.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1107.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.457468995670789
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRHL8fm8M4JCdswFmC+q8/5n4SrS5d:uITfip1SNMJfCUDW5d
MD5:	29C2797C5BA474C101A946E1AA47F4AA
SHA1:	570FA443DED89119AFC2D22F45294496ED66BC91
SHA-256:	3272A98333ACFFECFA08D650F065C2E2A6EB4F7B36980E483685A4DA519B1092
SHA-512:	46915D2F580C91F61936C2C34809644615BB9C8504D29D4438D6270073E1B387230BC6D2DEDDB658E9EDDB6B60F2221A872A9E3A97CE9F2A217EFEED849A1DD
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="943668" />.. <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\WER15C8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47560
Entropy (8bit):	2.0961769412214015
Encrypted:	false
SSDEEP:	192:xPaMVIAuBo1jsSqHhNjB49T0QAp2Q2iKQ2sjtpSwnLet:x0BovqBZG9hAplUsj9L+
MD5:	135EAA6FCF8D0245E54DFFD54941E8A9
SHA1:	2C7A40D97736AF36073837E50C5740F4803F342C
SHA-256:	D2D81873CEF781444295345AC822A4CE8D6D66DE7001E311245E1EAB613DCB7F
SHA-512:	F1789CECDEAA26BA3CBEE94C22BB7DC556F0F49F5E8702D05FBD984A8D913A10A5A83E21D83AAF5FC1039879CA3A18D7059E01003D4EFFEC153A6563BF04F268
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER177E.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):	8248
Entropy (8bit):	3.692388734375029
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigU6+6Yl+6ag5BgmfTBSYaCprRN89bSqsfSGm:RrlsNij6+6YM6aIgmfTBSYrqSJfK
MD5:	A53532775D62C1F08A3F36A33AFCD25F
SHA1:	5A7C07B3E6EF00BF910D39B96E2E0658A1D5BEAB
SHA-256:	A94274271F6DADDED36573B06CA12EBB6BE990CDEEC115A1001D37358D036856
SHA-512:	85953B709212AEDA948E402B6DEE210886F8B2D98867C29CC817A229D6D15CA6274293ECC1E45B571AD010DC1698C1616BC3F6F714C051D2D0D1D95F7E26FB4

C:\ProgramData\Microsoft\Windows\WER\Temp\WER177E.tmp.WERInternalMetadata.xml	
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.>.1.2.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER181B.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):	4.456077970284452
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRz8fm8M4JCdsnFPw45+q8/pr4SrSMd:uITfip1SNUJDwO6DWMd
MD5:	12308FC7EB3A734D70CA6A5641E7F082
SHA1:	C04106D3B1820F890F09B4F51D6AE7DB9DFEA31E
SHA-256:	0F7F71176446D2798557FA2FDB0607A6F60972039C187A438EF112BA123B9477
SHA-512:	060277EF0015E160394AABE22DF3F3D5C9AB6F024B49CF0EDBA12DDC12E67F047EABE0C50F83B1188ECC98C0B2A416EB204F074F706FB4D134A8159AEEC95F4F
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="943668" />.. <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\WER5949.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46156
Entropy (8bit):	2.115211313804719
Encrypted:	false
SSDEEP:	192://BbJDF9OI90nRthxcjB49T0QAeVBPIZzWnmfK:XpYRtjaG9hAePIZKaK
MD5:	8FA63BDDB9618163E58D6F89092D79EA
SHA1:	D4C8A273E1ECC9241367DC3926031970DD83DC26
SHA-256:	A3A39D4D1913826AFCB3D137110E5D595D957FD82471EC5E1EAEC48B62713951
SHA-512:	56C641CBD9E37E4C28CF74FF1386C52D2C6D0697C4E96C7F08DB86E034A6C06C287EBA72899651EBCCCF014790F61CBC53AA29A8C27D73557074C5D022C9DE6
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....L....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D61.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):	8248
Entropy (8bit):	3.6926364982583566
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLr6AdI6YI66lmgmfTgSYaCpru89b6nsfb01em:RrlsNin6X6Yo6UgmfTgSYI6sfb6
MD5:	04C4F4F527742DD4B921AF2419D28D4C
SHA1:	3DD1C84D6B17F62D9656FF05E211FC2C4920520B
SHA-256:	11C61D43C2ACB27AAC2ED5E356C0A17B478E5BE8E674AC2C7908BABF8FDB8A06
SHA-512:	5D91DB67E16D7F9A4F90EE9894B4C7CE049DFED8269FA727A9B1EE54C2362049D249FBB6DEBA4963BFED98A76D02A92AF166DD6DF2F618020C381789DDEDA30E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D61.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.>.6.2.2.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E2D.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):	4.456868111783803
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BR78fm8M4JCds8F3C+q8/pT4SrSod:uITfip1SNkJ0CKDWod
MD5:	1ABBFB49D46E7F7CD2A5D43D75B1A4FE
SHA1:	CDE14F5EB5309A9515DAB274294C73E6D99BF8FC
SHA-256:	C30CE647DF6730687F14B9225FD23A7F28EE01B0C1EBD6A187A6D557F068FF8F
SHA-512:	D2D94BCAD9F234263DBCA97DFB9D3FFC43A935A1232054420D3515AF71F02B3645765C454BDF98667DDBD8EEC422B70130EE786EC6F285AD8DEB41EB62CA22
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="943668" />.. <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\WER964.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:37 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	52204
Entropy (8bit):	2.0760074592212834
Encrypted:	false
SSDEEP:	192:98DXGBlnAti/tQAGhbLPzxotXtj+em14bgm8lgnTi:RlAgQAGFHmHj+EbT2
MD5:	077C4C61C47DA8414160687840B322A0
SHA1:	15A821EEBA4BD32ADE6BA6C4A0B5C6F7700757D1
SHA-256:	4131A17D0F987BF6A5DEA1BD9A3BA484FDFA5F1396E16A9DB1A9E7B7E1004377
SHA-512:	D08530924F60D4878E8EB7165CBFB7A632740F5ED58427B7D947E59823273BFE8FBC209100F9C881E732A6C9DC918574C91459D4CA8E310550D523AC164C9908
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....l.....GenuineIntelW.....T.....@....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:23 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47824
Entropy (8bit):	2.031695947274906
Encrypted:	false
SSDEEP:	192:L6z3ouCvUvp/BA5RnTsvajB49T0QAA+ro62Q6USLXNb:c36Mvp/l1TnG9hAAVQ6tz9
MD5:	8DF414F6FCF7C22D51C373A18FEC34CE
SHA1:	3A07F9B392B1D45BEB9275F9D8C2643068E4E676
SHA-256:	30B83FB043EC6DDADEADE22A87A24C192AF73C44E2299CC88E317E342A9AB89A
SHA-512:	8F2744D410202D2650E84BF00BF272226B5E1033F86AD3BDA748035CC70FE80D9B03B205AA96C1B7281926E802E9892FC39D5F3E762EFBEC269585FE53E10E70
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:23 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	51912
Entropy (8bit):	2.026857221534779
Encrypted:	false
SSDEEP:	192:ACqZVKWjauYv+XPzxotXtjzsNZGnuYseWnjoA:uZVpauO+7mHjz+GnuREA
MD5:	81A185BA6265E2D57556D14DE9AB9551
SHA1:	557EBAED35228613069794AE01A45F3A70F8FBDA
SHA-256:	4762A16C1AF657610030E11EDED1B8B82CAF6D77870C03C00C342D76D2AEFDE6
SHA-512:	C6AC056E515AD64E5A99108EE6457876AFF97204060797F5E91F1AF2FB4C7AE00B2C556F7597454D34A13F766223D2023070ADDC98B0E04B3A4E491EAA666F11
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....l.....GenuineIntelW.....T.....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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):	8238
Entropy (8bit):	3.6886133556067975
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXO6Fh6Ylg6625BgmfT5SYaCprF89b5nasfETm:RrlsNi+6T6Yi67gmfT5SYg5n5ft
MD5:	5AD4332490E4D6A684E2F4D70A9CC8D8
SHA1:	030E8E9CB7B186BDBC1F6E25FF7B72C9CB546DF5
SHA-256:	E6208855953B8C2D4C85916F927D598ED8FA8B426E3F89ACF83FB42A29BF09B5
SHA-512:	827B0AB0447DC7F213E8F11C6B8F43AA7C1F118BBCA1270710718B4C5827FE3B2444C3F9270BA00D8575BD6296B003818016B05A79CD3D3031CCF89210357451
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.>.4.6.0.<./.P.i.d. >.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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):	8236
Entropy (8bit):	3.690729134128786
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMR6T6YHf6DgmfT5SYaCprR389b5nosfwTm:RrlsNiq6T6Y/6DgmfT5SYro5nbfJ
MD5:	43A9442D48A90C9653155C8255A8FA38
SHA1:	0D2D51BCC8B56A57B6A54F90DFBAED1FD5912E22
SHA-256:	887E8C455527B7F174B43D446C1C89E761A00A75132C652C2EA3D5E5F4451CE0
SHA-512:	C2F5A29AAFEDEFD38296F8C7DC6C1882E67C017DCC4333AA4D986748BC574526ECAE4BF4F666A681C4D10820C68194553C5F4B35A1826F5B5C8065066222DDI
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.>.9.0.8.<./.P.i.d. >.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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):	4.454715130110772
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRa8fm8M4JCdsHFg+q8/pe4SrSjd:uITfip1SNDJUDDWjd

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.xml	
MD5:	F9F18283F0F0871DE351918D1D423B38
SHA1:	B53E18FEC130A5FAFDDEF8658153A9D334F5DFC7
SHA-256:	A8460D83BF8A2EABEF318715D959C1DAC0DDB72A8D3B1562E479999B67EC6AC0
SHA-512:	95324641A33B92A4A101DD1710B0B13B91AFFD25815522099B12A95578C298BDFBD4BECF7DC7AF6F0F82F444C868344C0968A4ECA09FC3BA69D779729ED0E03
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="943668" />.. <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\WERD92F.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):	4.457204122894694
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BR18fm8M4JCdsHFV+q8/pn4SrSYd:uITfip1SNmJh6DWYd
MD5:	F749AB0BAB15344712559D3E40E27C4C
SHA1:	1AB1F7687073462002BE4F842B846E57D0E76526
SHA-256:	4A91B9A9D85498492017A9789F853655BC99996B1E5DDDE16C814757296B7AEB
SHA-512:	80CE493FB24310BC9205F23D3CFC3217F87569B3D5763E316BBB3FD9049DBAB856683F91AF2F0BD50AC9629279AEF1699634D8709315668ACD29268C537DFDE(
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="943668" />.. <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\WERE179.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48412
Entropy (8bit):	2.4236105120867473
Encrypted:	false
SSDEEP:	192:9Puon2vsesUbP5ugjmY/ZzjB49T0QAE+r+GoBkn2sAo:p7VuPIImY/pG9hAEQoCrV
MD5:	897C1EB44B0EFC32C65E0C6AD76BCC2B
SHA1:	265AE04C276679CEB837D27EF8774F5564F2EA3D
SHA-256:	9C2E4AEA995E32B7A7A894180FC737492BDADE7DA715BBC3A6227ED13A7CE53A
SHA-512:	EE0FC70892A99695B6B74F72506F67FB85866D80735916B4001FD46EC1F07CEDBBDCEEDFE9AC0FD669123C1BCE29941A0D4A8A1B3193DAFF30F81F8EFBA49F E6
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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):	8256
Entropy (8bit):	3.692219645923817
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiS+6S6YlD6i5BgmfT9SYaCprI89bUOsfvxcm:RrlsNiL6S6Yh6KgmfT9SYHUNfv/
MD5:	1A62481E32DF7C5A5D8D395E66352573
SHA1:	CC1C66F8972C189F39BA972008386E3ABACFEC87
SHA-256:	1BA3748C8C0C092EA96AA0B3EE8214D418DDA7127AE9BCA974BA18C3D7E5BBE4
SHA-512:	0A053BE53F67F479F648ECCCE0970D89FE766099E09C6F0829D27BE7102B63FEB30FCD568CE21A5821EBDF5CAF3BCC604D6B8FD41F37BA180B53E469FD7DCA E4
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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.>.4.1.2.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.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):	4.4587604010172806
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRlM8fm8M4JCdszFXWP+q8/pNb4SrSOd:uITfip1SNpxJHWP4DWOd
MD5:	5B338868161B2751E14C6F2158DE8A93
SHA1:	F8370DDF34C20C3033F9ADA0D66956C40D561917
SHA-256:	91C243B18CACF7CFD449894D4277AB4ED6BE2B7D9E0E2257284438CD74BEB7C2
SHA-512:	34DA1375647EF86737186BED4103A9541CBCC429821CA522FB53B78C15B6A3E2E66892A78F9F8A50EBBF2DA64B8CA44E6C2D29D61E3529C777C818BAB7D5EDC
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="943668" />.. <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\WEREE1B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:29 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49456
Entropy (8bit):	2.324936217516685
Encrypted:	false
SSDEEP:	192:2DERcEoz2XzRJ6ErhCdgcKdpE+NlrjB49T0QADPWjsGt+rE0Xn8:LRhzRJHc7gpE+vXG9hADPWz+78
MD5:	B117A59DB3F5FFCFC16D855D6D25B665
SHA1:	802E437B2D0F5F14D5D295C9F5DC69C68BF6A0DA
SHA-256:	EE3C6E83309796BDC6E0E73AAFA34A576AE62AE0FD96C711022041A328B03758
SHA-512:	9BAE73528023D3BC1B06B38BCB6CE6A244AE742B30CBB2B64E072B1405DC52914306F8C40A1ADAF81BF1CF63498A20947194A0CC7DB092D12AA10568AA7372FB
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....<....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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):	8248
Entropy (8bit):	3.692832842021345
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZY6e1S6YlL685BgmfT9SYaCprRN89bjasfDhm:RrlsNi26e1S6Yp6EgmfT9SYrqj5f4
MD5:	0011F324F914930CE390B49420411144
SHA1:	758D23B80151DE2FD9F3C2D23B173FDE8FF7DD64
SHA-256:	C7B313F5C94AB2774F40EC901763EA4C4DDE5ED1ABFFA578BCC86B0CCB26AB05
SHA-512:	57F11D3F964B4FF59C22381F47B4A980FD29259783B6B4D9D0DAD4395086890C66332C773AF6036A72D316BD6C4D1DBD09ECBE74FF8471793BFBEF05298DCD8
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.>.5.4.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.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):	4.45638562939769
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRf8fm8M4JCdszFUC+q8/p94SrSBd:uITfip1SNgJkCUDWBd
MD5:	C47970AC16B5DC011F3759220E165DED
SHA1:	0EFEEDD1281456C765351929629AB335C5099D83
SHA-256:	2C12085780753121E5305963D8A157CC4C76E6820D49B50B78F228E531B15FB7
SHA-512:	6100FB43AB7758515EDFBB92F5C52581A4795C3FAFD34EFF7BC8309B0B817050AC81EB7D4A9005B3F962A5188BB28F952D713ADAC13F3BEEF5A9F3B492E50E69
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="943668" />.. <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\WERFA70.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Apr 12 22:37:32 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49468
Entropy (8bit):	2.32448379060306
Encrypted:	false
SSDEEP:	192:EIPKJMEJtDfQbY7MPErHXJJ+5qYygXhTkJxnf4LjB49T0QABhNzWDShVRfnKA7:NKBJtod8LXJJgNXhTy6G9hABhNKWhbP7
MD5:	859038BA02D9EB3D82EB95D1BE73CB2D
SHA1:	4E2A21E1C37F30A72F4E9B576D177F1A8E357DA9
SHA-256:	3DBB2C3299FCB4C2EBCDAADF0A3B8BBB38D42C2277C5254B5379C56C2B3968BF
SHA-512:	8957FAA8FDF20D4D0067C7141C0628D533F4187F5A4E8DD5E34FD26C2BB92659B205E022C7C2FBEB1BE18001814CAB43E54B14430F050A67F03686724C67233F
Malicious:	false
Preview:	MDMP..... .....t`.....U.....B.....<.....GenuineIntelW.....T.....d.....t`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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):	8244
Entropy (8bit):	3.691837329981628
Encrypted:	false
SSDEEP:	192:RrI7r3GLNipHJ676YlN6S5BgmfT2SYaCprC89bh+sfrLm:RrlsNipp676Yf66gmfT2SYJh9fm
MD5:	303909D69682068BF5E8E4FC53E5CBC0
SHA1:	500FBE3BE6BB4DE5DADD026BE9015881A8535FA0
SHA-256:	69A9250299F214507011B1067447CEB2FD1B1D445191090BCBF2964C2101B665
SHA-512:	4BC0377F2988742D301457C221D6A831C1D20D931DE66C26DA0F4C501D9D45781417B68B6BE473DE5B3F069C3BD65E398D9AB0DAB3FE9B4ECF5F01F3F1EB32D
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.>.5.9.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.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):	4.455031873638163
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.tmp.xml	
SSDEEP:	48:cvIwSD8zsdiJgtWI9C8WSC8BRpq8fm8M4JCdsiFqL+q8/pg4SrSFd:uITfip1SNlfJD5DWFd
MD5:	ED34800C5DB1A915DD8A0F80CD306374
SHA1:	4D54CE8D339E40D3FC191BFEC8E1D07FDE60A401
SHA-256:	7E3C158DC7A9FE153DE41BDE609D46DCBF6AC1ABB1518997CDCA13E3CDC911F8
SHA-512:	AC0FCA0C98C8D83E183634692183BF765601FBDE1A9AD99AE9623C3640D1A2ECBF1DE6DA2FF290E4FFDD6D2F894E2A6995DB8B48DC28427F615FFE29A8FC3E3E
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="943668" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.246113418766052
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:	59d2ed9608ac543bd671da7b17558ebce275f64dd80fc84abd10fd31dea49c5e
SHA512:	f37f6eaf9f234fbe93619c72e7e012fb37b6b5779ff80c244fc19bd3bb628b0193d275c3e7f21d168fcb0f994a49c61169b11fde30819543092d09b41283903d
SSDEEP:	3072:+KEDvFkRNFycul5xjfMEOlL9M0Uiu+SeiMEvqrWB37d7YM1t7OrGsLZQm:2vF1fIL9M0UiuheZEyrWBrhYMzOrGOT
File Content Preview:	MZ.....@.....!..L.!This 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

General

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	• 5/3/2015 5:00:00 PM 5/7/2016 4:59:59 PM
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 00007F2DC8E46DEBh
cmp dword ptr [1002ED14h], 00000000h
jmp 00007F2DC8E46E08h
cmp esi, 01h
je 00007F2DC8E46DE7h
cmp esi, 02h
jne 00007F2DC8E46E04h
mov eax, dword ptr [1002F444h]
test eax, eax
je 00007F2DC8E46DEBh
push edi
push esi
push ebx
call eax
test eax, eax
je 00007F2DC8E46DEEh
push edi
push esi
push ebx
call 00007F2DC8E46CCCh
test eax, eax
jne 00007F2DC8E46DE6h
xor eax, eax
jmp 00007F2DC8E46E30h
push edi
push esi
push ebx
call 00007F2DC8E324C6h
cmp esi, 01h
mov dword ptr [ebp+0Ch], eax
jne 00007F2DC8E46DEEh

Instruction
test eax, eax
jne 00007F2DC8E46E19h
push edi
push eax
push ebx
call 00007F2DC8E46CA8h
test esi, esi
je 00007F2DC8E46DE7h
cmp esi, 03h
jne 00007F2DC8E46E08h
push edi
push esi
push ebx
call 00007F2DC8E46C97h
test eax, eax
jne 00007F2DC8E46DE5h
and dword ptr [ebp+0Ch], eax
cmp dword ptr [ebp+0Ch], 00000000h
je 00007F2DC8E46DF3h
mov eax, dword ptr [1002F444h]
test eax, eax
je 00007F2DC8E46DEAh
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 00007F2DC8E46DEFh
test eax, eax
jne 00007F2DC8E46DF0h
cmp dword ptr [1002ED24h], 01h
jne 00007F2DC8E46DE7h
call 00007F2DC8E4B222h
push dword ptr [esp+04h]
call 00007F2DC8E4B252h
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

Name	Virtual Address	Virtual Size	Is in Section
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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 15:37:23.776918888 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:23.825750113 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:24.070734024 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:24.119632006 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:26.444294930 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:26.503865004 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:29.556344986 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:29.609024048 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:32.758222103 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:32.807192087 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:35.368165016 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:35.440346003 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:36.116631031 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:36.174431086 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:37.256149054 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:37.308007956 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:37.837579966 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:37.897800922 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:37.926729918 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:37.975469112 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:38.354058981 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:38.402890921 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:39.676330090 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:39.725358963 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:40.847671032 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:40.896512032 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:45.495614052 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:45.545123100 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:46.699636936 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:46.748308897 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:47.149960995 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:47.225677967 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:48.022911072 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:48.074620008 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:49.700583935 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:49.749530077 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:50.856734991 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:50.905729055 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:52.339027882 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:52.390705109 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:53.093946934 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:53.152700901 CEST	53	58987	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:37:57.678445101 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:57.727410078 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 15:37:58.847767115 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:37:58.904966116 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:00.414699078 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:00.466526031 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:01.019088030 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:01.077980042 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:01.310767889 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:01.362205982 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:02.305921078 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:02.355874062 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:04.202950954 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:04.251912117 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:04.353370905 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:04.365056038 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:04.415431976 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:04.419857025 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:04.667881966 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:04.728338957 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:05.506933928 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:05.555906057 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:07.002561092 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:07.060362101 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:07.235048056 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:07.283976078 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:07.901146889 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:07.959809065 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:10.202023983 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:10.250639915 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:11.025602102 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:11.074461937 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:13.193722963 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:13.245479107 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:13.395973921 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:13.444628954 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:14.225234032 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:14.299627066 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:14.556699991 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:14.605465889 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:15.448067904 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:15.501127005 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:16.365973949 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:16.414992094 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:22.344455004 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:22.396333933 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:22.420856953 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:22.469569921 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:23.232795000 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:23.294663906 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:25.565232992 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:25.622898102 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:45.531151056 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:45.579962015 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:47.469578028 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:47.519100904 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 12, 2021 15:38:55.438565969 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:38:55.487325907 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:05.805751085 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:05.873660088 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:06.354765892 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:06.411943913 CEST	53	61633	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:07.203736067 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:07.283396006 CEST	53	55949	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:40:07.666245937 CEST	57601	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:07.725917101 CEST	53	57601	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:08.168935061 CEST	49342	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:08.262109041 CEST	53	49342	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:08.702919006 CEST	56253	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:08.762516975 CEST	53	56253	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:09.129040003 CEST	49667	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:09.281012058 CEST	53	49667	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:09.845436096 CEST	55439	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:09.903076887 CEST	53	55439	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:10.691759109 CEST	57069	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:10.754353046 CEST	53	57069	8.8.8.8	192.168.2.3
Apr 12, 2021 15:40:11.133805037 CEST	57659	53	192.168.2.3	8.8.8.8
Apr 12, 2021 15:40:11.191056967 CEST	53	57659	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:38:04.667881966 CEST	192.168.2.3	8.8.8.8	0x7298	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:37:35.440346003 CEST	8.8.8.8	192.168.2.3	0xeabf	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:37:36.174431086 CEST	8.8.8.8	192.168.2.3	0xac9a	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:37:37.308007956 CEST	8.8.8.8	192.168.2.3	0xf0a5	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:37:37.897800922 CEST	8.8.8.8	192.168.2.3	0xa66f	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:38:04.728338957 CEST	8.8.8.8	192.168.2.3	0x7298	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- loaddll32.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe

rundll32.exe
rundll32.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 3664 Parent PID: 5768

General

Start time:	15:37:20
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:	0x1030000
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: 4080 Parent PID: 3664

General

Start time:	15:37:20
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:	0xbd0000
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: 460 Parent PID: 3664

General

Start time:	15:37:21
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,CPUSpeed
Imagebase:	0x880000
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: 908 Parent PID: 4080

General

Start time:	15:37:21
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\utility.dll',#1
Imagebase:	0x880000
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: 5360 Parent PID: 460

General

Start time:	15:37:22
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 460 -s 688
Imagebase:	0x370000
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	6DEC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_149cdf75	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_149cdf75\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CE0.tmp.csv	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D00.tmp.txt	success or wait	1	6DEB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a3 cb 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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 cc 01 00 00 a0 cb 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U..........B......<..... ..GenuineIntelW...........T... ....t`................. ....0..1............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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 1c f6 37 00 76 01 11 00 00 00 00 00 54 f6 37 00 f6 19 00 10 23 00 00 00 46 02 01 00 10 f6 37 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...+. ..+................7.v....... T.7.....#...F.....7.+.........	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	168	e0 03 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 76 01 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	....v........... ....$..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	20	0e 00 00 00 d8 c7 94 02 00 00 00 00 04 00 00 00 f2 30 00 00	................0..	success or wait	14	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	4	4c f8 7a 00	L.z.	success or wait	13	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	6636	bc 9a e5 77 a3 1a 21 75 aa aa aa aa 48 e8 37 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 ac 02 00 00 a8 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 f0 40 00 00 00 00 00 00 00 00 00 00 00 00 00 48 e8 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..!u....H.7............... ....$........... .... @.............H.7.............	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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 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 1c f6 37 00 aa aa aa aa 00 00 00 00 a8 e7 37 00 bc 9a e5 77 23 00 00 00 06 02 00 00 18 e6 37 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...+. ..+................7......... ..7....w#.........7.+.........	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	48	b4 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 80 41 00 00 00 00 00 68 f6 82 00 00 00 00 00 98 09 00 00 1a 6e 00 00 cc 02 00 00 42 2d 00 00	....A.....h..... ....n......B-..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.tmp.dmp	unknown	752	00 00 48 74 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 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 04 00 00 00 00 40 83 02 00 00 00 00 00 80 a2 02 00 00 00 00 73 1e 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 f7 46 03 00 00 00 00 00 1f 47 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 8c 1b 00 00 00 00 00 0d 73 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 dd 04 00 00 00 00	..Ht.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....@..... s.....F.....G .....3.....s..... @.....@.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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.....l.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD60F.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 e4 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 68 1b 00 00 b0 9f 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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	28	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.6.0.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 35 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.>.2.4.5.9.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.5.0.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 39 00 39 00 32 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.>.8.4.9.9.2.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 39 00 39 00 32 00 30 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.>.8.4.9.9.2.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.6.1.5.2.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.8.8.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 39 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.2.9.6.1.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 30 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.3.0.4.3.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 39 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.2.9.6.1.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.6.6.4.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 35 00 32 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.>.3.0.5.2.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 38 00 36 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.>.8.6.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 30 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.0.3.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 34 00 37 00 31 00 36 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.>.6.4.7.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 68 00 6b 00 66 00 6a 00 75 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.h.k.f.j.u.e.,. .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 68 00 6b 00 66 00 6a 00 75 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.k.f.j.u.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 32 00 30 00 33 00 31 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.>.1.5.7.2.0.3.1.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 33 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.2.2.:.3.7.:.2.3.Z.".>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	256	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 36 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 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 00 3e	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.8.". .P.I.D.=.".4.6.0.". .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 34 00 30 00 35 00 61 00 32 00 32 00 31 00 2d 00 33 00 61 00 33 00 33 00 2d 00 34 00 38 00 36 00 38 00 2d 00 39 00 65 00 35 00 30 00 2d 00 62 00 65 00 38 00 65 00 61 00 36 00 33 00 30 00 62 00 30 00 65 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.4.0.5.a.2.2.1.-.3.a.3.3.-.4.8.6.8.-.9.e.5.0.-.b.e.8.e.a.6.3.0.b.0.e.4.<./.G.u.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 33 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.2.2.:.3.7.:.2.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_149cdf75\Report.wer	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_149cdf75\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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_149cdf75\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 34 00 31 00 30 00 34 00 36 00 31 00 30 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.6.4.1.0.4.6.1.0.1.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DED1FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 F6 19 00 10 02 00 00 00 01 00 00 00 76 01 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DED1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 1956 Parent PID: 908

General

Start time:	15:37:22
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 908 -s 696
Imagebase:	0x370000
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	6DEC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_07c90a00	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_07c90a00\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp	success or wait	1	6DEB497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD833.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92F.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92F.tmp.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D7E.tmp.csv	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D9E.tmp.txt	success or wait	1	6DEB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a3 cb 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.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 6c 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 8c 03 00 00 a1 cb 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B.....I..... ..GenuineIntelW.....T... .....t`..... .....0..1..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.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 6c fa ba 02 7c 00 0f 00 00 00 00 00 a4 fa ba 02 f6 19 00 10 23 00 00 00 46 02 01 00 60 fa ba 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	....+...S...+. ..+..............l...|....... ....#...F...`...+.........	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	168	78 02 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 7c 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 0e 25 00 00	x............................ ....|........... ....%..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	20	11 00 00 00 00 fd ec 02 00 00 00 00 00 03 00 00 1e 34 00 00	................4..	success or wait	17	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	768	bc b1 e5 77 d6 c9 e3 77 64 02 00 00 aa aa aa aa 10 00 00 00 94 fd ec 02 60 fe ec 02 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 20 c9 02 00 20 c9 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 20 c9 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 e4 05 03 00 00 00 00 00 00 00 00 38 06 06 03 00 c0 c8 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 98 fa 03 03 54 c2 c8 02 a0 fa 03 03 d0 04 06 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 00	...w...wd...............`..... ..@..w@..w..... ... .d... ....d........ ....8....................... ....T.	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	4	3c f7 1c 03	<...	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.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 6c fa ba 02 aa aa aa aa 00 00 00 00 f8 eb ba 02 bc 9a e5 77 23 00 00 00 02 02 00 00 68 ea ba 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...+. ..+...............l........... ....w#.......h...+.........	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	48	64 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 80 c9 02 00 00 00 00 70 f6 1c 03 00 00 00 00 90 09 00 00 ba 4d 00 00 cc 02 00 00 3e 30 00 00	d....... ....p..... ....M......>0..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 f4 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 a0 83 02 00 00 00 00 00 80 a2 02 00 00 00 00 79 1e 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 20 47 03 00 00 00 00 00 24 47 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 81 8d 1b 00 00 00 00 00 bf 71 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 dd 04 00 00 00 00	..Ht.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... .... y..... G.....$G .....q..... @.....@.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD63E.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 1c 15 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 0a 33 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 58 af 00 00 15 00 00 00 ec 01 00 00 e8 1c 00 00 16 00 00 00 98 00 00 00 d4 1e 00 00	....3.....T.....8..... ....T.....X.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	28	3c 00 50 00 69 00 64 00 3e 00 39 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.9.0.8.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 35 00 39 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.>.2.5.9.3.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 35 00 34 00 36 00 30 00 34 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.>.1.2.5.4.6.0.4.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 35 00 34 00 35 00 32 00 32 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.>.1.2.5.4.5.2.2.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 30 00 33 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.5.0.3.2.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 30 00 33 00 32 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.5.0.3.2.9.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 35 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 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.>.2.6.5.5.2.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.6.2.8.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 38 00 36 00 32 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.>.5.3.8.6.2.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 39 00 34 00 34 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.>.5.3.9.4.4.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 38 00 36 00 32 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.>.5.3.8.6.2.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.0.8.0.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 30 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.>.2.9.0.8.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 31 00 35 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.5.0.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 30 00 32 00 37 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.>.3.7.0.2.7.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 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.>.3.4.1.1.9.6.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.3.5.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.1.1.9.6.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 68 00 6b 00 66 00 6a 00 75 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.h.k.f.j.u.e.,. .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 68 00 6b 00 66 00 6a 00 75 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.k.f.j.u.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 32 00 30 00 33 00 31 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.>.1.5.7.2.0.3.1.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 33 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.2.2.:.3.7.:.2.3.Z.".>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	256	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 39 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 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 00 3e	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.9.". .P.I.D.=.".9.0.8.". .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 64 00 30 00 63 00 61 00 32 00 61 00 35 00 2d 00 37 00 66 00 65 00 62 00 2d 00 34 00 34 00 35 00 31 00 2d 00 61 00 62 00 61 00 66 00 2d 00 35 00 36 00 62 00 62 00 37 00 33 00 31 00 64 00 33 00 36 00 64 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.d.0.c.a.2.a.5.-.7.f.e.b.-.4.4.5.1.-.a.b.a.f.-.5.6.b.b.7.3.1.d.3.6.d.6.<./.G.u.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 33 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.2.2.:.3.7.:.2.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8A1.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92F.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_07c90a00\Report.wer	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_07c90a00\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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1a1eb18902f2cde56c230bea1f2d46b66fdcaf_82810a17_07c90a00\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 34 00 30 00 30 00 31 00 32 00 37 00 36 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2.4.0.0.1.2.7.6.1.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEB43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6DED36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6DED36BF	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 76 01 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7C 00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DED1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 4120 Parent PID: 3664

General

Start time:	15:37:24
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:	0x880000
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: 5816 Parent PID: 4120

General

Start time:	15:37:25
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4120 -s 688
Imagebase:	0x370000
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	6DEC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_16d4e8ad	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_16d4e8ad\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp	success or wait	1	6DEB497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.tmp.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER787D.tmp.csv	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER788D.tmp.txt	success or wait	1	6DEB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a6 cb 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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 18 10 00 00 a4 cb 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B.....<..... ..GenuineIntelW.....T... .....t`..... .....0..1..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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 89 00 00 00 00 00 16 1d 72 01 80 1d 72 01 74 ec b5 02 74 ec b5 02 20 f0 a8 04 5f f1 00 10 23 00 00 00 46 02 01 00 44 ec b5 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	....+...S...+. ..+....@........r...r.t...t... ..._...#...F...D...+.........	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	168	ac 06 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 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	20	11 00 00 00 44 dc b5 02 00 00 00 00 bc 23 00 00 22 31 00 00	....D........#.."1..	success or wait	17	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	9148	bc 9a e5 77 a3 1a 21 75 aa aa aa aa 78 de b5 02 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 ac 02 00 00 a8 02 00 00 00 00 00 00 24 00 00 00 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 aa aa aa aa 00 b0 de 02 00 00 00 00 00 00 00 00 00 00 00 00 00 78 de b5 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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..!u....x................ ....$........... ....x..............	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	4	80 fc 10 03	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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 00 00 00 00 aa aa aa aa 74 ec b5 02 00 00 00 00 d8 dd b5 02 bc 9a e5 77 23 00 00 00 06 02 00 00 48 dc b5 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	?............................ ....+...S...+. ..+..................t....... ....w#.......H...+.........	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	48	94 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 df 02 00 00 00 00 b4 fb 10 03 00 00 00 00 4c 04 00 00 de 54 00 00 cc 02 00 00 42 2d 00 00	....@........... ..L.....T......B-..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.tmp.dmp	unknown	752	00 00 48 74 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 00 40 41 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 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 e0 70 02 00 00 00 00 00 80 a2 02 00 00 00 00 5c 21 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 f0 47 03 00 00 00 00 00 aa 48 03 00 00 00 00 00 00 00 00 00 00 00 00 00 b7 60 1b 00 00 00 00 00 89 9e 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 dd 04 00 00 00 00	..Ht.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....p..... \!.....G.....H .....`..... @.....@.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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 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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE179.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 14 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 fc a1 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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 31 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.1.2.0.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.1.2.3.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 35 00 38 00 32 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.>.1.4.9.2.5.8.2.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 35 00 30 00 30 00 34 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.>.1.4.9.2.5.0.0.4.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 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.>.8.4.3.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 33 00 39 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.2.7.3.9.3.2.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 33 00 39 00 33 00 32 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.>.3.2.7.3.9.3.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 36 00 31 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.>.2.1.6.1.4.4.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 38 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.>.2.1.5.8.7.2.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 37 00 37 00 32 00 31 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.>.2.9.5.7.7.2.1.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 38 00 35 00 34 00 30 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.>.2.9.5.8.5.4.0.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 37 00 37 00 32 00 31 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.>.2.9.5.7.7.2.1.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.6.6.4.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 37 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.>.5.9.7.4.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 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.>.9.0.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 34 00 37 00 31 00 36 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.>.6.4.7.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 68 00 6b 00 66 00 6a 00 75 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.h.k.f.j.u.e.,. .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 68 00 6b 00 66 00 6a 00 75 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.k.f.j.u.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 32 00 30 00 33 00 31 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.>.1.5.7.2.0.3.1.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 32 00 32 00 3a 00 33 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.2.2.:.3.7.:.2.6.Z.".>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 34 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 31 00 32 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 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.=.".3.4.6.". .P.I.D.=.".4.1.2.0.". .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 35 00 66 00 31 00 61 00 30 00 38 00 38 00 2d 00 39 00 65 00 35 00 30 00 2d 00 34 00 37 00 31 00 32 00 2d 00 62 00 30 00 37 00 33 00 2d 00 61 00 34 00 33 00 66 00 33 00 63 00 66 00 62 00 36 00 34 00 64 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.5.f.1.a.0.8.8.-.9.e.5.0.-.4.7.1.2.-.b.0.7.3.-.a.4.3.f.3.c.f.b.6.4.d.0.<./.G.u.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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 32 00 32 00 3a 00 33 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.2.2.:.3.7.:.2.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE36E.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE42A.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_16d4e8ad\Report.wer	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_16d4e8ad\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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_16d4e8ad\Report.wer	unknown	42	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 30 00 32 00 39 00 35 00 35 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.6.0.2.9.5.5.1.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEB43D1	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 F6 19 00 10 02 00 00 00 01 00 00 00 7C 00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5F F1 00 10 02 00 00 00 00 00 00 00 00 40 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DED1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 5436 Parent PID: 3664

General

Start time:	15:37:27
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:	0x880000
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: 5512 Parent PID: 5436

General

Start time:	15:37:28
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5436 -s 688
Imagebase:	0x370000
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	6DEC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_15e4f4b3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f8892833bb6a965bb21678f4e1a_82810a17_15e4f4b3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.tmp.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84C3.tmp.csv	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84D4.tmp.txt	success or wait	1	6DEB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a9 cb 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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 3c 15 00 00 a7 cb 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 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B.....<..... ..GenuineIntelW.....T... ....<.....t`..... .....0..1..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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 89 00 00 00 00 00 95 1a 25 00 80 f0 30 04 ec eb 43 00 ec eb 43 00 20 f0 30 04 5f f1 00 10 23 00 00 00 46 02 01 00 bc eb 43 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+....@........%...0...C...C. .0._...#...F.....C.+.........	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	168	0c 11 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 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	20	12 00 00 00 60 e7 1c 00 00 00 00 00 04 00 00 00 32 31 00 00	....`...........21..	success or wait	18	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	4	dc 95 e5 77	...w	success or wait	17	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	4096	68 f8 fa 03 00 00 fb 03 00 40 fa 03 00 00 00 00 00 1e 00 00 00 00 00 00 00 70 36 00 00 00 00 00 3c 15 00 00 ac 13 00 00 00 00 00 00 00 00 00 00 00 e0 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 d6 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	h........@...............p6..... <.................5......... ....p.w..............	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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 ec eb 43 00 00 00 00 00 50 dd 43 00 bc 9a e5 77 23 00 00 00 16 02 00 00 c0 db 43 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...+. ..+.....................C..... P.C....w#.........C.+.........	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	48	ac 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 36 00 00 00 00 00 bc f6 fa 03 00 00 00 00 44 09 00 00 06 5a 00 00 cc 02 00 00 42 2d 00 00	....p6........... ..D....Z......B-..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.tmp.dmp	unknown	752	00 00 48 74 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 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 80 70 02 00 00 00 00 00 80 a2 02 00 00 00 00 cf 21 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 b6 4d 03 00 00 00 00 00 c8 4d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 8d 1b 00 00 00 00 00 8c 71 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 dd 04 00 00 00 00	..Ht.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....p..... .!.....M.....M .....q..... @.....@.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE1B.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 10 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.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.3.6.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 36 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.0.6.0.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 37 00 34 00 33 00 34 00 37 00 35 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.>.1.2.7.4.3.4.7.5.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 37 00 34 00 32 00 36 00 35 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.4.2.6.5.6.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 33 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.1.1.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 31 00 30 00 39 00 38 00 35 00 34 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.9.8.5.4.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 31 00 30 00 39 00 38 00 35 00 34 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.9.8.5.4.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 34 00 35 00 33 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 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.>.4.5.3.2.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 34 00 35 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.5.0.5.6.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 37 00 37 00 32 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.7.2.9.1.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 37 00 37 00 33 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.7.3.7.3.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 37 00 37 00 32 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.7.2.9.1.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.6.6.4.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 31 00 36 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.9.1.6.1.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 33 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.3.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 34 00 37 00 31 00 36 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.>.6.4.7.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 68 00 6b 00 66 00 6a 00 75 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.h.k.f.j.u.e.,. .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 68 00 6b 00 66 00 6a 00 75 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.k.f.j.u.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 32 00 30 00 33 00 31 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.>.1.5.7.2.0.3.1.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 39 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.2.2.:.3.7.:.2.9.Z.".>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 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 33 00 37 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.=.".3.5.0.". .P.I.D.=.".5.4.3.6.". .U.p.t.i.m.e.M.S.=.".3.7.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.7.4.". .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 35 00 36 00 31 00 65 00 33 00 64 00 66 00 2d 00 39 00 37 00 30 00 37 00 2d 00 34 00 63 00 38 00 36 00 2d 00 39 00 35 00 30 00 37 00 2d 00 34 00 62 00 31 00 64 00 36 00 38 00 37 00 34 00 31 00 62 00 34 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.5.6.1.e.3.d.f.-.9.7.0.7.-.4.c.8.6.-.9.5.0.7.-.4.b.1.d.6.8.7.4.1.b.4.f.<./.G.u.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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 32 00 32 00 3a 00 33 00 37 00 3a 00 32 00 39 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.2.2.:.3.7.:.2.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD2.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF06F.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_15e4f4b3\Report.wer	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_15e4f4b3\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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8e1c7dc65b4f88928 33bb6a965bb21678f4e1a_82810a17_15e4f4b3\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 39 00 32 00 34 00 37 00 34 00 36 00 34 00 33 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.9.2.4.7.4.6.4.3.9.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED36BF	unknown
\REGISTRY\A\{d04ed78e-15f2-226f-c877-9a6844414d3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEB43D1	unknown

Analysis Process: rundll32.exe PID: 5988 Parent PID: 3664

General

Start time:	15:37:30
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:	0x880000
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: 5352 Parent PID: 5988

General

Start time:	15:37:31
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5988 -s 688
Imagebase:	0x370000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	6DEC1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEB497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.tmp	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.tmp.xml	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9139.tmp.csv	success or wait	1	6DEB4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9159.tmp.txt	success or wait	1	6DEB4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 ac cb 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....t`.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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 64 17 00 00 aa cb 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B.....<..... ..GenuineIntelW.....T... ....d.....t`..... .....0..1..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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 d8 eb 67 00 22 01 15 00 38 00 00 00 00 00 00 00 0e 00 00 00 38 00 00 00 28 ec 67 00 e0 ae 00 10 23 00 00 00 02 02 01 00 c0 eb 67 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...+...+.....g."...8...........8...(.g.....#.........g.+...	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	168	7c 01 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 ae 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 01 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 de 24 00 00	|.."..$..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	20	11 00 00 00 28 fb 95 02 00 00 00 00 d8 04 00 00 22 31 00 00	....(..........."1..	success or wait	17	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	1240	bc b1 e5 77 d6 c9 e3 77 5c 02 00 00 aa aa aa aa 10 00 00 00 bc fb 95 02 88 fc 95 02 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 b0 45 00 00 b0 45 00 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 b0 45 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 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 60 07 9c 02 00 00 00 00 00 00 00 00 50 07 9b 02 00 20 45 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 22 45 00 ac f7 8d 02 e8 05 9b 02 b4 f7 8d 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	...w...w\..................... ..@..w@..w......E...E.....\... ....\.........E.............. ....`...........P.... E................ ....T"E...	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	2336	bc b1 e5 77 d6 c9 e3 77 5c 02 00 00 aa aa aa aa 10 00 00 00 74 f7 8d 02 40 f8 8d 02 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 80 45 00 00 80 45 00 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 80 45 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 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 e0 c7 9a 02 00 00 00 00 00 00 00 00 50 07 9b 02 00 20 45 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 f4 fb 95 02 54 22 45 00 fc fb 95 02 e8 05 9b 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	...w...w\...........t...@..... ..@..w@..w......E...E.....\... ....\.........E.............. ....P.... E................ ....T" E............................	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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 00 00 00 00 aa aa aa aa 00 00 00 00 58 dd 67 00 bc 9a e5 77 23 00 00 00 02 02 00 00 c8 db 67 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	?............................ ....+...S...+. ..+.......................... X.g....w#.........g.+.........	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	48	74 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 b0 45 00 00 00 00 00 28 fb 95 02 00 00 00 00 d8 04 00 00 22 31 00 00 cc 02 00 00 42 2d 00 00	t....... ....E.....(..... ......"1......B-..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	4	32 00 00 00	2...	success or wait	50	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.tmp.dmp	unknown	752	00 00 48 74 00 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 04 00 00 00 00 e0 6a 02 00 00 00 00 00 80 a2 02 00 00 00 00 9c 22 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 39 4d 03 00 00 00 00 00 e2 4d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e3 97 1b 00 00 00 00 00 5d 67 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 dd 04 00 00 00 00	..Ht.....0...U..s@...$..... .....B.....B?..... .....#..... ..@A.....Zb..... ....j..... ."..... .....9M.....M .....]g..... @.....@.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA70.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 14 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 1c 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.....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.8.8.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 35 00 30 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.>.1.9.5.0.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.5.0.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 31 00 34 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.5.1.1.4.8.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 31 00 34 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.5.1.1.4.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.6.0.8.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 38 00 31 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.>.2.5.8.1.6.<./.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 35 00 39 00 32 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.2.5.9.2.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 36 00 37 00 34 00 35 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.>.5.2.6.7.4.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 35 00 39 00 32 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.2.5.9.2.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.6.6.4.<./.P.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 33 00 31 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.>.1.2.3.1.8.<./.U.p.t.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.6.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 34 00 37 00 31 00 36 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.>.6.4.7.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 35 00 39 00 33 00 39 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.>.5.9.3.9.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 68 00 6b 00 66 00 6a 00 75 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.h.k.f.j.u.e.,. .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 68 00 6b 00 66 00 6a 00 75 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.k.f.j.u.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 32 00 30 00 33 00 31 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.>.1.5.7.2.0.3.1.6.8.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 32 00 32 00 3a 00 33 00 37 00 3a 00 33 00 32 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.2.2.:.3.7.:.3.2.Z.".>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 38 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 37 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 33 00 37 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.=.". 3.5.4.". .P.I.D.=.".5.9.8.8.". .U.p.t.i.m.e.M.S.=.".3.7.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.7.4.". .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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 35 00 39 00 38 00 33 00 31 00 66 00 35 00 2d 00 61 00 31 00 65 00 64 00 2d 00 34 00 32 00 31 00 36 00 2d 00 62 00 39 00 38 00 36 00 2d 00 37 00 33 00 33 00 36 00 63 00 37 00 30 00 65 00 62 00 39 00 66 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.5.9.8.3.1.f.5.-.a.1.e.d.-.4.2.1.6.-.b.9.8.6.-.7.3.3.6.c.7.0.e.b.9.f.8.<./.G.u.i.d.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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 32 00 32 00 3a 00 33 00 37 00 3a 00 33 00 32 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.2.2.:.3.7.:.3.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFC65.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	6DEB497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD02.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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146\Report.wer	unknown	2	ff fe	..	success or wait	1	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146\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	6DEB497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3cc1cbeb22cf5bba1b683f1de9c66cedfb1a534_82810a17_14850146\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 2d 00 32 00 39 00 31 00 35 00 38 00 37 00 31 00 38 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.9.1.5.8.7.1.8.9.	success or wait	1	6DEB497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4928 Parent PID: 3664

General

Start time:	15:37:34
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:	0x880000
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: 3580 Parent PID: 4928

General

Start time:	15:37:35
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4928 -s 688
Imagebase:	0x370000
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: 1268 Parent PID: 3664

General

Start time:	15:37:37
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:	0x880000
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: 3512 Parent PID: 1268

General

Start time:	15:37:38
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1268 -s 688
Imagebase:	0x370000
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: 3352 Parent PID: 3664

General

Start time:	15:37:40
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:	0x880000

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: 5716 Parent PID: 3664

General

Start time:	15:37:44
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:	0x880000
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: 5324 Parent PID: 3664

General

Start time:	15:37:47
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:	0x1310000
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: 3544 Parent PID: 3664

General

Start time:	15:37:50
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:	0x1f0000
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: 6220 Parent PID: 3664

General

Start time:	15:37:53
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\utility.dll,DirectoryAdd
Imagebase:	0x1f0000
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: 6332 Parent PID: 6220

General

Start time:	15:37:55
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6220 -s 688
Imagebase:	0x1380000
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: 6356 Parent PID: 3664

General

Start time:	15:37:57
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:	0x1f0000
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: 6444 Parent PID: 3664

General

Start time:	15:38:00
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:	0x1f0000
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