



ID: 356831
Sample Name:
executable.4420.exe
Cookbook: default.jbs
Time: 17:38:41
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report executable.4420.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 11
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 13
Data Directories 13
Sections 13
Imports 13
Network Behavior 14
UDP Packets 14
Code Manipulations 15
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: executable.4420.exe PID: 5412 Parent PID: 5608 16

General 16
File Activities 16
File Created 16
Registry Activities 16
Key Value Created 16
Analysis Process: WerFault.exe PID: 2100 Parent PID: 5412 17
General 17
File Activities 17
File Created 17
File Deleted 17
File Written 18
Registry Activities 40
Key Created 40
Key Value Created 40
Disassembly 41
Code Analysis 41

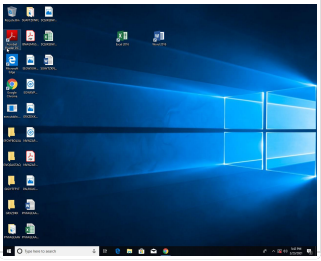
Analysis Report executable.4420.exe

Overview

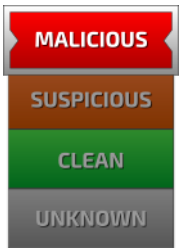
General Information

Sample Name:	executable.4420.exe
Analysis ID:	356831
MD5:	6192cfbe8e44360.
SHA1:	166886066ffabb7..
SHA256:	8e353600579959..
Infos:	

Most interesting Screenshot:



Detection

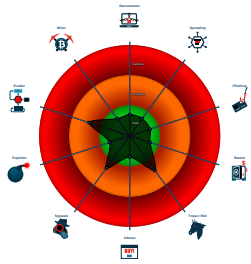


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Contains functionality for read data f…
- Contains functionality to download a…
- Contains functionality to dynamically…
- Contains functionality to open a port…
- Contains functionality to read the cli…
- Contains functionality to upload files…
- Found large amount of non-executed…
- Found potential string decryption / a…
- Monitors certain registry keys / valu…
- One or more processes crash

Classification



Startup

- **System is w10x64**
- executable.4420.exe (PID: 5412 cmdline: 'C:\Users\user\Desktop\executable.4420.exe' MD5: 6192CFBE8E44360F7C0B6F696206F41D)
  - WerFault.exe (PID: 2100 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5412 -s 672 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

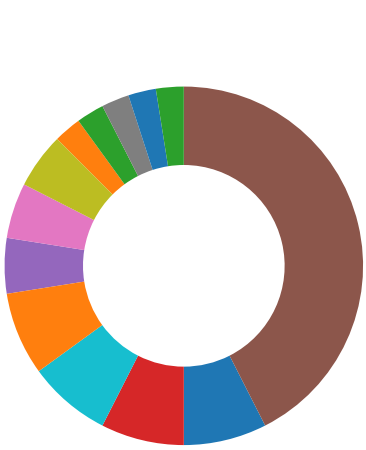
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking

Copyright null 2021



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:



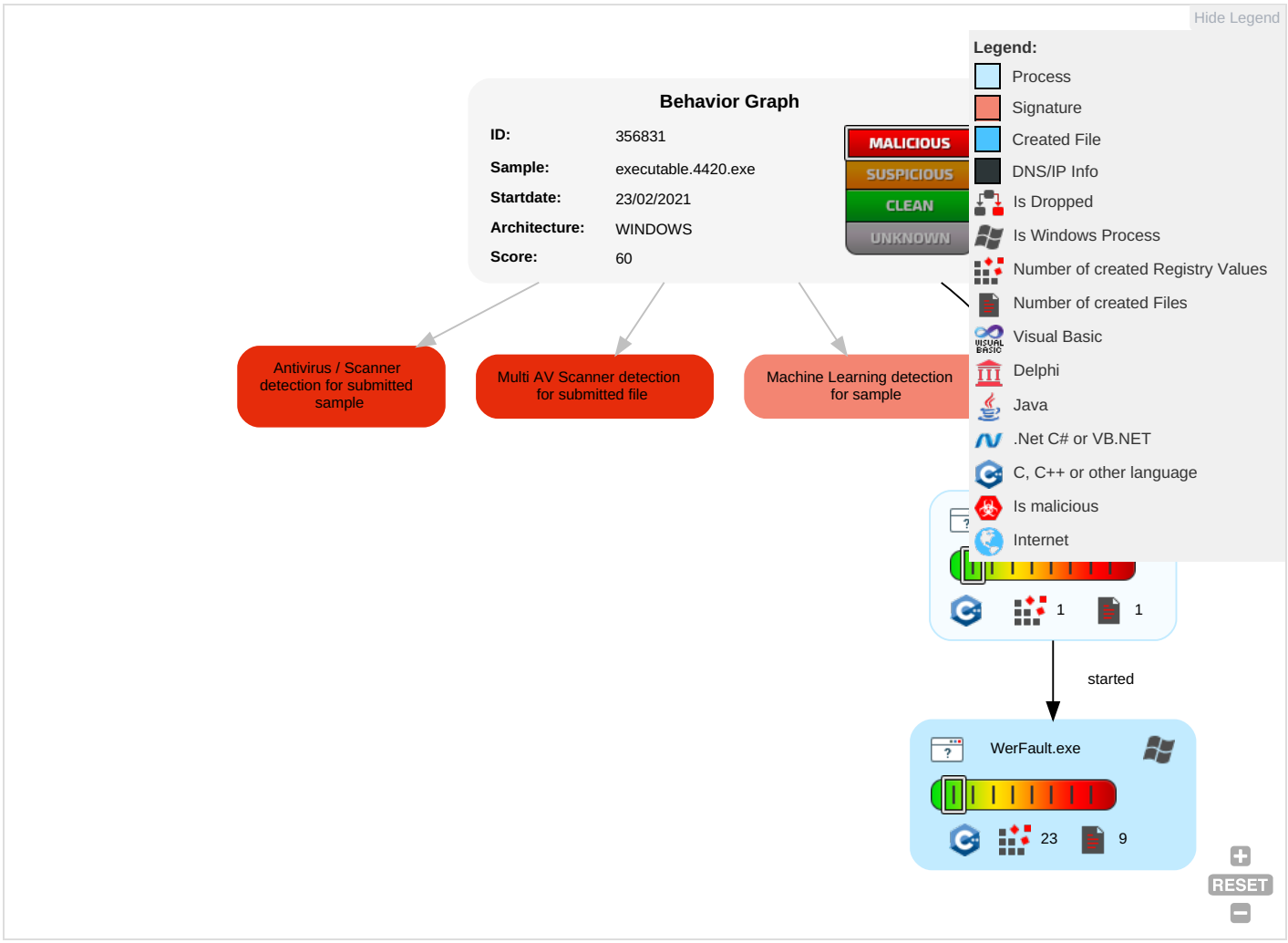
Uses 32bit PE files

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1 1	Remote Services	Clipboard Data 2	Exfiltration Over Alternative Protocol 1	Ingress Tool Transfer 1 1	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Copyright null 2021

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
executable.4420.exe	74%	ReversingLabs	Win32.Spyware.Perfect	
executable.4420.exe	100%	Avira	HEUR/AGEN.1112545	
executable.4420.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.executable.4420.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1112545		Download File
0.0.executable.4420.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1112545		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.blazingtools.com/update.tmpupdates/bpk.dat	0%	Avira URL Cloud	safe	
http://www.blazingtools.com/orderbpk.html_This	0%	Avira URL Cloud	safe	
http://www.blazingtools.com/downloads.html	1%	Virustotal		Browse
http://www.blazingtools.com/downloads.html	0%	Avira URL Cloud	safe	
http://www.blazingtools.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.blazingtools.com/update.tmpupdates/bpk.dat	executable.4420.exe	false	• Avira URL Cloud: safe	unknown
http://www.blazingtools.com/orderbpk.html_This	executable.4420.exe	false	• Avira URL Cloud: safe	unknown
http://www.blazingtools.com/downloads.html	executable.4420.exe	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.blazingtools.com/	executable.4420.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356831
Start date:	23.02.2021
Start time:	17:38:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	executable.4420.exe
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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winEXE@2/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 90.1%) • Quality average: 71.8% • Quality standard deviation: 31.1%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 23.211.6.115, 104.43.193.48, 40.88.32.150, 52.255.188.83, 184.30.24.56, 51.11.168.160, 8.250.157.254, 8.248.95.254, 8.238.27.126, 8.241.80.126, 8.248.123.254, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

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_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11694
Entropy (8bit):	3.7672748277627535
Encrypted:	false
SSDEEP:	192:h/5h7gBgH/UJuLl+7jpLPAz/u7ssS274ItM/1c:tz/UJuLcjCz/u7ssX4It0c
MD5:	7A55A9DC34D7C94401B8ED3160BA0C72
SHA1:	F4AE306D576E833E6A99A8363306C07D9DD76A06
SHA-256:	35E4069BB231E06A148487DCAC11D00BE8A891927E7CC072221A7056F001F51C
SHA-512:	9B3C9B7EA90710D5C183686C7CB6977E33357DE869B25ED2D18182B7F94D65BE3CBD209640AE7837043826B243424205AF3939D4D7704BB80C276E5AF9D212E8
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.6.0.4.3.7.6.4.4.2.6.1.1.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.6.0.4.3.7.8.8.3.3.2.3.4.0.....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.=.0.d.0.3.d.2.5.1.-.e.c.9.b.-.4.4.e.9.-.a.4.6.d.-.7.a.f.5.b.0.9.4.0.5.a.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.d.a.6.f.5.f.1.-.d.3.f.7.-.4.9.a.e.-.b.2.e.f.-.b.9.2.1.0.9.a.6.f.9.5.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.e.x.e.c.u.t.a.b.l.e...4.4.2.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.2.4.-.0.0.0.1.-.0.0.1.7.-.f.7.1.d.-.3.7.e.7.4.d.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.7.b.e.2.9.9.c.7.9.9.4.b.9.5.3.7.7.c.d.6.2.c.1.5.c.1.9.9.9.1.9.0.0.0.0.f.f.f.f.!.0.0.0.0.1.6.6.8.8.6.0.6.6.f.f.a.b.b.7.6.f.6.b.7.2.c.4.b.4.e.d.9.1.f.a.1.9.e.5.9.9.8.7.a.!.e.x.e.c.u.t.a.b.l.e...4.4.2.0...e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 24 01:39:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1080022
Entropy (8bit):	1.2269964489942033
Encrypted:	false
SSDEEP:	3072:eS293HEp5CUPF0iJTiSQCidYakBWg+vSsThybQv:eS29X65CUPF0iJTiSQCidYakEg+v9Qbm
MD5:	B9A9BEE69F8163C259E82977694A384E
SHA1:	500E77B794EB34E6B0A50D43FA8D767CE220D611
SHA-256:	EF357D66AA69B8ECAE3AA51BA7FF633B2C709DB23F74EEA1FC236F6C60018722
SHA-512:	018C33E5506E918DF09B1F4859D22AB2D97D5D3A53F85A0736CD1BDADA2C64CDD87862BDBD7158FDF6749D7744CA220BF54C595B2521C6ECADECC955DB9C 1B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....X.5`.....U.....B.....GenuineIntelW.....T.....$...U.5`.....0..2.....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\WER655E.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):	8320
Entropy (8bit):	3.693017369135634
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUWV68nw6YSeSUh2sLgmfXlZS/LNCpDs89bXnisf79m:RrlsNiV68nw6YbSUh2ogmfLS/LsXnhfM
MD5:	C9E60060870D3B974BE4AFC5F943DBB3
SHA1:	66BFC2EE917214F25A0C603029918D30BCB8913F
SHA-256:	918D1EE2E7E2C757290948589858F1515FAC4E694A7236A4D155E0CD1971CE61

C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	
SHA-512:	AE855276116DCF22E25C23D3D800C4F974AC71C6A2C2AF10EEA556FC4D3F3F3D1413890BCD796B556B9A9DDEB0A5980F88DCEC3FB2C6AF56BAA568AFF42FECB
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4597
Entropy (8bit):	4.461112344435761
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjtJgtWI9LrWSC8BT8fm8M4JSHd8lFb+q8r3Y70UHj+d:uITfjHYaSNyJS987q3+DHj+d
MD5:	5D91C01CE7A87CC544F3B72FE1EB4DD3
SHA1:	5E7E5241C6400239CB4406316B6AF0FE2FF95FF4
SHA-256:	E6BA6B6FBB2687EBA4F1DEE10D64EE7B7AB566032F570DB75477951426E4CA36
SHA-512:	99990EB14ED48B65E833CF3F67CE36E24912B5DBE627BE1AC8340D8BB7970D10593D05634FE7290EACE6311B042C2690EB720E197B5786DA8057BDDDD2E596F7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874730" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	3.300468788976393
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	executable.4420.exe
File size:	438272
MD5:	6192cfbe8e44360f7c0b6f696206f41d
SHA1:	166886066ffabb76f6b72c4b4ed91fa19e59987a
SHA256:	8e353600579959f0507d00376d2e56e8c9a24648b2574ee72fa81dec5d70874a
SHA512:	d492b9ea094bd6e695a562a855587feaf793be0cb35cf28df681a0022a8e0139a222a68bd578fb65b125fe9fea86f1f596bf337e65a445e8a5286d95ae037857
SSDEEP:	3072:U+NvJwwbI7mZgauugh+KsvkfGDLNj58E2wL6uEXKlwjwxhfgtRlh:9swbYmZgarrKsvVDR5POuE6lwqf4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u....R...R...R.].R...R.c.R...R.]>R...R.\.R...R.`.R...R\c.R...R.`.R...R.`.R...R.Y.R...R...R.}.R%\.R...R...R...R.Y.R...R.y.R...

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x43e7ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x47299316 [Thu Nov 1 08:49:26 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4dc9b0b4e019be52f23cc9a3c195910d

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0044A588h
push 0043E91Eh
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [00444824h]
pop ecx
or dword ptr [00455C18h], FFFFFFFFh
or dword ptr [00455C1Ch], FFFFFFFFh
call dword ptr [004447B4h]
mov ecx, dword ptr [00455BF8h]
mov dword ptr [eax], ecx
call dword ptr [00444754h]
mov ecx, dword ptr [00455BF4h]
mov dword ptr [eax], ecx
mov eax, dword ptr [00444758h]
mov eax, dword ptr [eax]
mov dword ptr [00455C14h], eax
call 00007F4964A1E080h
cmp dword ptr [004550A0h], ebx
jne 00007F4964A47B0Eh
push 0043E948h
call dword ptr [0044475Ch]
pop ecx
call 00007F4964A47C05h
push 00453078h
push 00453074h
call 00007F4964A47BF0h
mov eax, dword ptr [00455BF0h]
mov dword ptr [ebp-6Ch], eax

Copyright null 2021

Instruction
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [00455BECh]
lea eax, dword ptr [ebp-64h]
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [00444764h]
push 00453070h
push 00453000h
call 00007F4964A47BBDh

Rich Headers

Programming Language:	• [C++] VS98 (6.0) SP6 build 8804 • [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x50b58	0x154	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x56000	0x14cf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x44000	0xaa0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x42469	0x43000	False	0.261452746035	COM executable for DOS	3.69971850757	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x44000	0xeb80	0xf000	False	0.221451822917	data	3.38138099515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x53000	0x2c20	0x3000	False	0.368815104167	data	4.63470137622	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x56000	0x14cf8	0x15000	False	0.0564778645833	data	0.900735057676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
WININET.dll	FtpPutFileA, InternetConnectA, FtpSetCurrentDirectoryA, FtpCreateDirectoryA, InternetOpenA, InternetGetConnectedState, InternetCloseHandle
MFC42.DLL	
MSVCRT.dll	__p__commode, _adjust_fdiv, __setusermatherr, _initterm, __getmainargs, _acmdln, exit, _XcptFilter, _exit, ?terminate@@YAXXZ, _except_handler3, _onexit, __dllonexit, ??1type_info@@UAE@XZ, getenv, strrchr, atoi, _ftol, time, difftime, fabs, floor, strcat, srand, __p__fmode, _stricmp, fopen, fwrite, fclose, strchr, memmove, strncpy, setlocale, isspace, _splitpath, _makepath, strcpy, _strlwr, strstr, wcscmp, strcmp, strncmp, malloc, free, sscanf, strlen, sprintf, _purecall, _CxxThrowException, memcpy, memset, __CxxFrameHandler, __set_app_type, rand, _itoa, wcslen, _setmbcp, _controlfp

DLL	Import
KERNEL32.dll	CloseHandle, FlushViewOfFile, ReleaseMutex, WaitForSingleObject, CreateFileMappingA, MapViewOfFile, CreateMutexA, CreateFileA, DeviceIoControl, GetFileSize, MulDiv, lstrlenA, lstrcmpA, lstrcpynA, GlobalReAlloc, GlobalHandle, UnmapViewOfFile, LoadResource, LockResource, GlobalAlloc, GlobalFree, GlobalLock, GlobalUnlock, FindFirstFileA, GetComputerNameA, GetDateFormatA, GetTimeFormatA, GetVersionExA, OpenProcess, GetCurrentThreadId, WideCharToMultiByte, lstrlenW, MultiByteToWideChar, SetCurrentDirectoryA, SetFileTime, GetSystemTime, GetStartupInfoA, InterlockedDecrement, GetProcAddress, LoadLibraryA, FreeLibrary, lstrcpyA, ReadFile, WriteFile, lstrcmpiA, DeleteFileA, GetTimeZoneInformation, SetLastError, Sleep, GetTickCount, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, FileTimeToSystemTime, SetFilePointer, GetFileInformationByHandle, SystemTimeToFileTime, GetLocalTime, CreateProcessA, lstrcatA, EnumResourceNamesA, CopyFileA, GetTempFileNameA, GetTempPathA, LocalFree, FormatMessageA, GetLastError, SizeofResource, RemoveDirectoryA, MoveFileA, CreateDirectoryA, GetSystemDirectoryA, GetModuleFileNameA, GetModuleHandleA, ExpandEnvironmentStringsA, GetCurrentProcessId, FindClose, FindResourceA, FindNextFileA
USER32.dll	GetDlgItemInt, GetDlgItemTextA, MessageBoxA, SetForegroundWindow, FindWindowA, GetWindowTextA, SetClipboardViewer, PostQuitMessage, ChangeClipboardChain, SetMenuDefaultItem, EnableMenuItem, wsprintfA, RegisterHotKey, UnregisterHotKey, LoadImageA, FillRect, DrawTextA, PtInRect, CharLowerA, GetWindowThreadProcessId, AttachThreadInput, CloseClipboard, GetClipboardData, OpenClipboard, IsClipboardFormatAvailable, IsWindowUnicode, LoadStringA, CharUpperBuffA, RedrawWindow, SetWindowLongA, InvalidateRect, MessageBeep, GetDlgCtrlID, DdeFreeStringHandle, IsWindowVisible, GetClassNameA, SendMessageTimeoutA, IsWindow, RegisterWindowMessageA, FindWindowExA, DestroyIcon, AppendMenuA, GetMenuItemCount, GetMenuItemInfoA, GetSubMenu, DrawFrameControl, OffsetRect, DrawIconEx, DrawEdge, GetSystemMetrics, SystemParametersInfoA, GetKeyboardLayout, MapVirtualKeyExA, MapVirtualKeyA, GetKeyNameTextA, EnumChildWindows, GetWindowLongA, IsDlgButtonChecked, GetForegroundWindow, PostMessageA, DdeClientTransaction, DdeGetData, GetSysColor, GetCursorPos, WindowFromPoint, GetCapture, GetWindowRect, GetFocus, InflateRect, CopyRect, DrawFocusRect, SetTimer, GetParent, GetWindowTextLengthA, GetNextDlgTabItem, SetFocus, GetDlgItem, CreatePopupMenu, CheckMenuItem, DdeCreateStringHandleA, GetKeyboardLayoutList, DdeConnect, SendMessageA, EnableWindow, GetDesktopWindow, GetDC, ReleaseDC, DdeFreeDataHandle, DdeDisconnect, DdeInitializeA, DdeUninitialize, KillTimer, DefWindowProcA, IsChild, LoadIconA, SetCursor, LoadCursorA, GetKeyboardLayoutNameA, GetClientRect
GDI32.dll	BitBlt, SelectObject, CreateCompatibleDC, CreatePen, CreateFontIndirectA, Rectangle, GetTextColor, CreateFontA, GetDIBits, CreateCompatibleBitmap, GetTextExtentPoint32A, CreateSolidBrush, SetTextColor, SetBkMode, DeleteDC, CreateDCA, GetStockObject, GetPaletteEntries, GetObjectA, CreateDIBitmap, CreatePalette, RealizePalette, PatBlt, DeleteObject, CreateBitmap
comdlg32.dll	GetOpenFileNameA
ADVAPI32.dll	RegOpenKeyA, RegSetValueExA, RegCreateKeyA, RegQueryValueExA, RegQueryValueA, RegDeleteValueA, RegCloseKey, RegDeleteKeyA, GetUserNameA, RegOpenKeyExA
SHELL32.dll	Shell_NotifyIconA, SHBrowseForFolderA, SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHGetMalloc, SHFileOperationA, ShellExecuteA, ExtractIconExA
COMCTL32.dll	ImageList_Remove, ImageList_GetImageCount, ImageList_ReplaceIcon, InitCommonControlsEx
ole32.dll	CoUninitialize, CoInitialize, CoCreateInstance, CoFreeUnusedLibraries
OLEAUT32.dll	SysStringLen, VariantInit, VariantClear, SysAllocString, SysFreeString
urlmon.dll	URLDownloadToFileA
WSOCK32.dll	send, recv, closesocket, select, connect, WSACleanup, ntohl, WSAStartup, htons, ioctlsocket, gethostbyname, bind, WSASetLastError, socket, gethostname
MSVCP60.dll	??0_Lockit@std@@QAE@XZ, ??1_Lockit@std@@QAE@XZ
RPCRT4.dll	UuidCreate, UuidToStringA, RpcStringFreeA

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:39:25.233937979 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:25.285471916 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:26.376651049 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:26.428426981 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:28.041127920 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:28.100127935 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:28.905944109 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:28.973481894 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:29.322885990 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:29.392126083 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:30.896219969 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:30.944962025 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:31.976865053 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:32.029597998 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:33.256689072 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:33.305219889 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:34.683229923 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:34.736665964 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:35.631702900 CET	58361	53	192.168.2.3	8.8.8.8

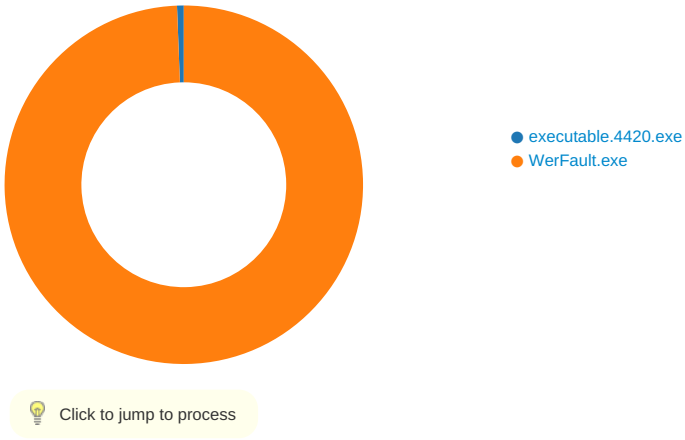
Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:39:35.680376053 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:36.559864044 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:36.617083073 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:37.945734978 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:37.994498968 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:39.115470886 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:39.164233923 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:39.239679098 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:39.288265944 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:40.260013103 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:40.308773994 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:41.080451965 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:41.129209995 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:42.294761896 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:42.354716063 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:43.181158066 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:43.232711077 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:44.147665024 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:44.196490049 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:45.087042093 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:45.135683060 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 17:39:58.153821945 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:39:58.212501049 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 17:40:05.136533022 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:40:05.185122967 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 17:40:18.742022038 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:40:18.799397945 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 17:40:27.437750101 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:40:27.509244919 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 17:40:46.809015036 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:40:46.857649088 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 17:40:52.416899920 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:40:52.480557919 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 17:41:21.967437983 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:41:22.018543959 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 17:41:23.779164076 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:41:23.839287043 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:21.578418970 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:21.638370037 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:22.242088079 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:22.302165985 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:22.883418083 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:22.943257093 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:23.421056032 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:23.480940104 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:24.035535097 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:24.092859030 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:24.596959114 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:24.646073103 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:25.192250013 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:25.252090931 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:25.980870962 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:26.029532909 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:27.071306944 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:27.119978905 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 17:42:27.595020056 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:42:27.652151108 CET	53	52123	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: executable.4420.exe PID: 5412 Parent PID: 5608

General

Start time:	17:39:33
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\executable.4420.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\executable.4420.exe'
Imagebase:	0x400000
File size:	438272 bytes
MD5 hash:	6192CFBE8E44360F7C0B6F696206F41D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BPK\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	420AD2	CreateDirectoryA

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer	IEPK	binary	56 AE 35 60 05 00 00 00	success or wait	1	41B11F	RegSetValueExA

Analysis Process: WerFault.exe PID: 2100 Parent PID: 5412

General

Start time:	17:39:35
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5412 -s 672
Imagebase:	0x7ff7488e0000
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	6DE41717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE3497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp	success or wait	1	6DE3497A	unknown

Copyright null 2021

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	success or wait	1	6DE34BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	success or wait	1	6DE34BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp.xml	success or wait	1	6DE34BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER948C.tmp.csv	success or wait	1	6DE34BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94AC.tmp.txt	success or wait	1	6DE34BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 58 ae 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....X.5`.....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.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 dc 1b 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 24 15 00 00 55 ae 35 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 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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... ....$...U.5`..... .....0..2..... 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	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	524288	00 00 00 00 52 dd e6 77 80 15 0a 00 a8 fe 19 00 d0 15 0a 00 08 15 0a 00 04 21 0a 00 70 dd e6 77 a8 fe 19 00 68 15 0a 00 24 dd e6 77 80 15 0a 00 a8 fe 19 00 d0 15 0a 00 08 15 0a 00 27 1e 44 00 d0 15 0a 00 80 15 0a 00 00 00 00 00 da 22 e5 77 80 15 0a 00 a8 fe 19 00 d0 15 0a 00 08 15 0a 00 27 1e 44 00 00 00 00 00 00 00 00 00 80 15 0a 00 00 00 00 00 a8 fe 19 00 aa aa aa aa a8 fe 19 00 aa aa aa aa aa aa aa aa aa 00 00 00 00 a8 fe 19 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	752	00 00 37 75 00 00 00 00 00 60 00 00 f9 0a 01 00 51 32 d9 44 9e 20 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 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 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 70 78 02 00 00 00 00 00 00 94 02 00 00 00 00 27 1d 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 f3 4c 03 00 00 00 00 00 f9 4c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 85 1b 00 00 00 00 00 cc 79 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 e3 dc 04 00 00 00 00	..7u.....`......Q2.D. ....B.......B?..... ...."..... ..@E.....Zb..... ....px..... '.....L.....L .....t.....y..... @.....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	10076	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	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D2F.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 bc 11 00 00 9c 07 00 00 05 00 00 00 24 01 00 00 e6 2b 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 40 1b 00 00 de 5f 10 00 15 00 00 00 ec 01 00 00 58 19 00 00 16 00 00 00 98 00 00 00 44 1b 00 00	.....$. ...+.....T.....8..... ....T.....@...._..... ..X.....D...	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.1.2.<./.P.i.d.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	84	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 65 00 63 00 75 00 74 00 61 00 62 00 6c 00 65 00 2e 00 34 00 34 00 32 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.e.c.u.t.a.b.l.e...4.4.2.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.7.2.0.<./.U.p.t.i.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 39 00 36 00 36 00 34 00 35 00 31 00 32 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.>.9.6.6.4.5.1.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 39 00 36 00 36 00 34 00 31 00 30 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.6.6.4.1.0.2.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 36 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.>.2.5.6.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 39 00 39 00 34 00 30 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.9.4.0.9.9.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 39 00 39 00 34 00 30 00 39 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.9.4.0.9.9.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 32 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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.>.1.8.2.5.8.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 32 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.2.5.8.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 33 00 31 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.5.7.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 33 00 31 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.4.4.0.<./.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 34 00 30 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.>.2.9.0.4.0.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 38 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.0.8.1.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 34 00 30 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.>.2.9.0.4.0.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 35 00 36 00 34 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.9.5.6.4.7.7.<./.U.p.t.i.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 32 00 39 00 33 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.>.4.2.9.3.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 30 00 38 00 33 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.0.8.3.4.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 37 00 33 00 31 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.>.1.0.3.7.3.1.2.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 31 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.1.4.2.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 32 00 37 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.2.7.5.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.5.0.4.<./.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 37 00 30 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.0.1.7.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 30 00 33 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.0.3.3.0.8.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 33 00 31 00 31 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.3.1.1.0.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 30 00 33 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.0.3.3.0.8.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 65 00 78 00 65 00 63 00 75 00 74 00 61 00 62 00 6c 00 65 00 2e 00 34 00 34 00 32 00 30 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.>.e.x.e.c.u.t.a.b.l.e...4.4.2.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 71 00 73 00 64 00 70 00 71 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.y.q.s.d.p.q.,. .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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 71 00 73 00 64 00 70 00 71 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.y.q.s.d.p.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 36 00 39 00 35 00 33 00 30 00 39 00 31 00 39 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.>.1.5.6.9.5.3.0.9.1.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.8.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 32 00 2d 00 32 00 34 00 54 00 30 00 31 00 3a 00 33 00 39 00 3a 00 33 00 38 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.-.0.2.-.2.4.T.0.1.:.3.9.:.3.8.Z.".>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 33 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 33 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 37 00 33 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.=.".3.3.8.". .P.I.D.=.".5.4.1.2.". .U.p.t.i.m.e.M.S.=.".7.3.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.3.4.". .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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 64 00 30 00 33 00 64 00 32 00 35 00 31 00 2d 00 65 00 63 00 39 00 62 00 2d 00 34 00 34 00 65 00 39 00 2d 00 61 00 34 00 36 00 64 00 2d 00 37 00 61 00 66 00 35 00 62 00 30 00 39 00 34 00 30 00 35 00 61 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.d.0.3.d.2.5.1.-.e.c.9.b.-.4.4.e.9.-.a.4.6.d.-.7.a.f.5.b.0.9.4.0.5.a.e.<./.G.u.i.d.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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 32 00 2d 00 32 00 34 00 54 00 30 00 31 00 3a 00 33 00 39 00 3a 00 33 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.4.T.0.1.:.3.9.:.3.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER655E.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	6DE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65FB.tmp.xml	unknown	4597	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39\Report.wer	unknown	2	ff fe	..	success or wait	1	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39\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	171	6DE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_08086b39\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 33 00 34 00 34 00 39 00 39 00 39 00 33 00 30 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.3.4.4.9.9.9.3.0.3.	success or wait	1	6DE3497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	success or wait	1	6DE536BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DE51FB2	RegCreateKeyExW
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE343D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	ProgramId	unicode	000677be299c7994b95377cd62c15c1999190000ffff	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	FileId	unicode	0000166886066ffabb76f6b72c4b4ed91fa19e59987a	success or wait	1	6DE536BF	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	LowerCaseLongPath	unicode	c:\users\user\desktop\executable.4420.exe	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	LongPathHash	unicode	executable.4420.|8ef1d93b	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	Name	unicode	executable.4420.exe	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	Publisher	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	Version	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	BinFileVersion	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	BinaryType	unicode	pe32_i386	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	ProductName	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	ProductVersion	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	LinkDate	unicode	11/01/2007 08:49:26	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	BinProductVersion	unicode		success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	Size	B	00 B0 06 00 00 00 00 00	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	Language	dword	0	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	IsPeFile	dword	1	success or wait	1	6DE536BF	unknown
\REGISTRY\A\{3b1e9e52-55c7-525f-27c4-0be9d0371a1c}\Root\InventoryApplicationFile\executable.4420.|8ef1d93b	IsOsComponent	dword	0	success or wait	1	6DE536BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 27 1E 44 00 02 00 00 00 01 00 00 00 00 00 00 00 00