ID: 356831
Sample Name:
executable.4420.exe
Cookbook: default.jbs
Time: 17:32:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

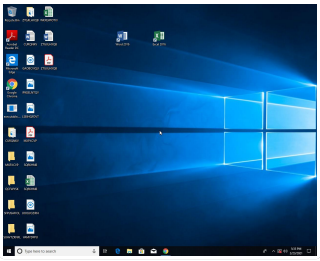
Analysis Report executable.4420.exe

Overview

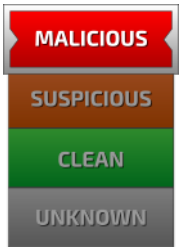
General Information

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

Most interesting Screenshot:



Detection

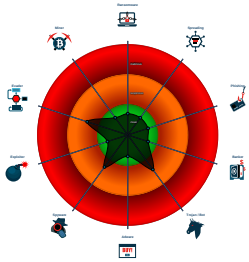


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 7112 cmdline: 'C:\Users\user\Desktop\executable.4420.exe' MD5: 6192CFBE8E44360F7C0B6F696206F41D)
  - WerFault.exe (PID: 5856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

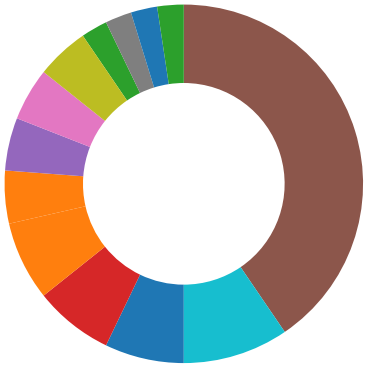
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Remote Access Functionality

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

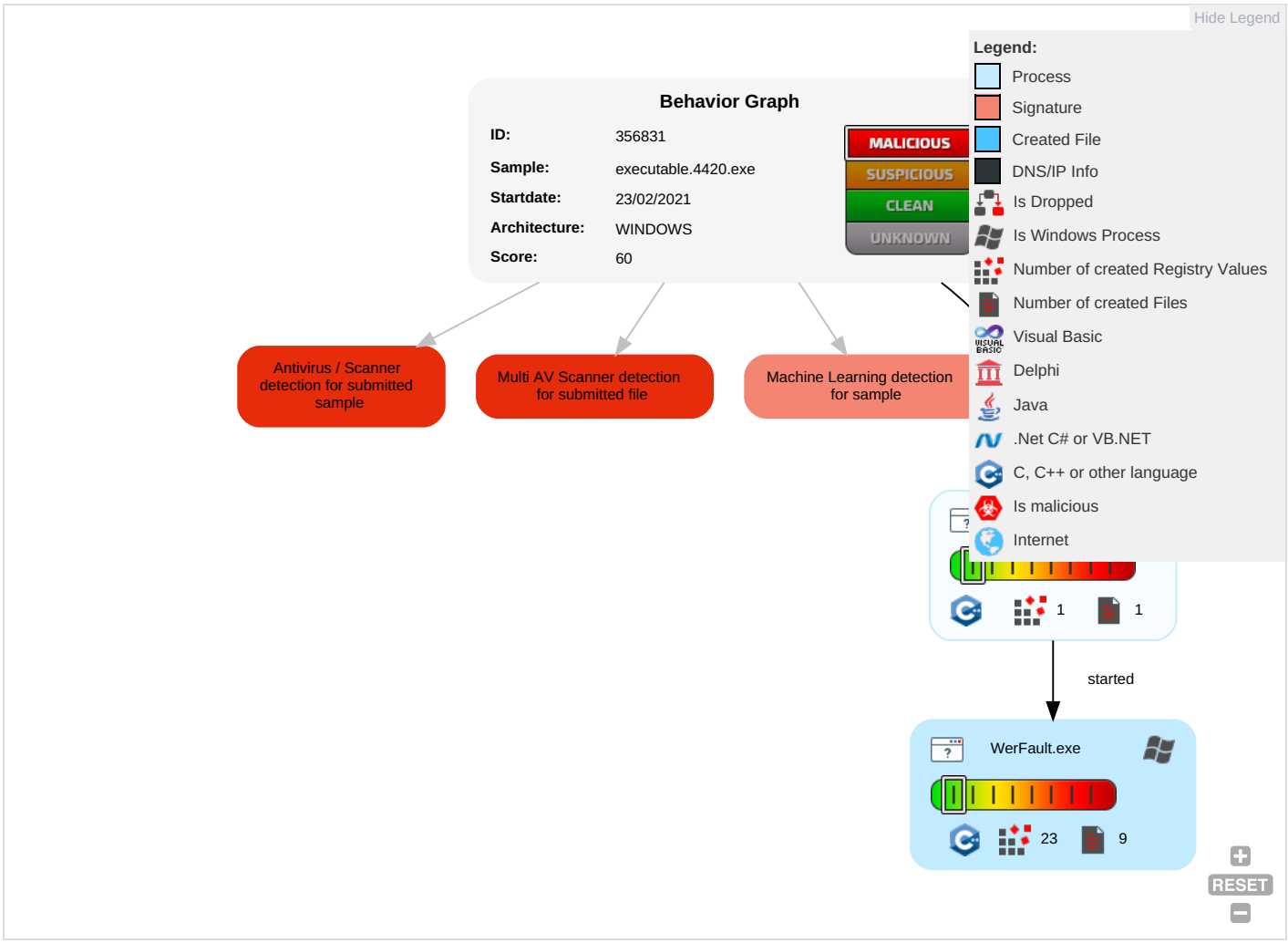
Binary contains paths to debug symbols

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 De Without Authoriz
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 Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software 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	Process 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User 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	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station	

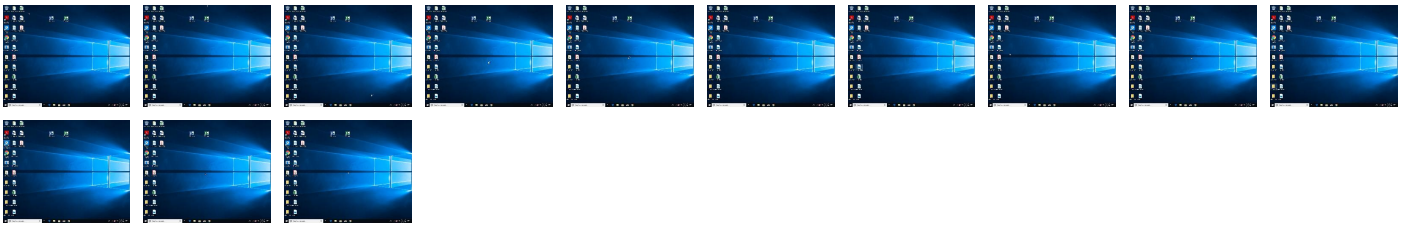
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	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	• Avira URL Cloud: safe	unknown
http://crl.microsoft	WerFault.exe, 00000004.0000000 3.682815138.0000000004ED6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: 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:	17:32:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
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
Number of analysed new started processes analysed:	20
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 • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 168.61.161.212, 13.107.246.254, 23.211.6.115, 52.147.198.201, 104.43.139.144, 13.64.90.137, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 8.248.121.254, 8.253.204.249, 8.248.143.254, 8.248.135.254, 8.248.119.254, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.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, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, t-ring.t-9999.t-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
17:33:15	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_168581 3a\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11726
Entropy (8bit):	3.769916385992574
Encrypted:	false
SSDEEP:	192:tJknh75BgH/UJuLVe7jBrPAz/u7sWS274ItMP1F:bMw/UJuLcjKz/u7sWX4It0F
MD5:	0C01155023A36D9E2DAB66E877103554
SHA1:	489051F8E0DB7A7AE8F00A4E4DCC53BF37E929F0
SHA-256:	D267EC28890985E2A14E447F22A79DDC147396886D78F9BEE3F72649BBF500FB
SHA-512:	9AA05053FF62920D4F2732F48FC5D7467B48A16C18FB8C5B19D0C3DD10A593C7DA1F459B57748ACB60EC9D37F7401A902A82CDA937CF8DC9D1DCA4D8269B54 E
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.=.1.3.2.5.8.5.7.1.5.8.4.6.7.0.9.8.4.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.5.7.1.5.8.9.9.3.6.5.8.6.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.3.8.f.0.4.6.0.-.3.5.8.3.-.4.b.3.7.-.9.f.3.9.-.8.6.3.4.b.6.2.8.c.3.d.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.a.4.4.7.3.3.0.-.1.2.9.a.-.4.7.f.a.-.b.6.f.2.-.7.4.a.e.f.4.0.2.8.8.c.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.b.c.8.-.0.0.0.1.-.0.0.1.b.-.f.a.c.f.-.b.1.8.c.0.1.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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\WER5865.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Feb 23 16:33:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	1085526
Entropy (8bit):	1.2210534980162013
Encrypted:	false
SSDEEP:	1536:VcpPfIY/EnrIqBkTiRcO3kkP3nFHBjf2rLk/p17:EgY/tEksVxMrLG7
MD5:	9EA8D8935DD62708B6F7A878CD221E88
SHA1:	999D1845B7B1D709ED65F7DE307E1D26D8168202
SHA-256:	6B3D0461EF3C94BE23362456530AF2703A71753E66390AA1D6B051C3A8308066
SHA-512:	CFD1974D3A8D4280AF8BCE8BA28A605488E27F819A086C535526AB1BD5A8F35E6D03137F9E2B0A2F88A66505C574FA4B2B326E386EEC7C9C83693606FB134BF
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....A.5`.....U.....B.....GenuineIntelW.....T.....<.5`.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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):	8316
Entropy (8bit):	3.6945173129731437
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNixWA6JB2T6YrpSUwW8/gmfXlZS/LM+pD089bKbKsfNkkjm:RrlsNin6v2T6YlSUwWUgmfLS/LZKbpfk
MD5:	1FCC27E2DD05A24687AC7AF559479613
SHA1:	161D62CBD1DA5B6AD0B8469B6CDFF5DE3FB6656D
SHA-256:	A3295E86AF60BE69C6DDFA7961E2EA4CA8153201008146D6A1AA5CFCE435D3BB
SHA-512:	D72CD49A3BED6214C6FB9E597C0375D3DF726A5094E826353E6F5C329C046AFB88D98357B18CC354EADC375189B134B5EE667B3A6DE6D80EA1A7938A39861B 3
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.>.7.1.1.2.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.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):	4.455068962408137
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9JUkWSC8Bh8fm8M4JSHd8lFr+q8r3Y7wFUHjTd:uITfruU9SN4JS98Lq3+w+HjTd
MD5:	3C9F716FF3820EC27E2BF1DA7EA405D0
SHA1:	1F64446E6CB07224DDB7B6A3C9D6147816623211
SHA-256:	09570CC72E66EF66B1635A9BCC109BFF750049B603A673CCB74F7810B3F9C914
SHA-512:	0EF9AEEAE7120A5302C7493137F31F8E1EAAF7B9AB793A6098DB7EAC068192DA302A32A0BC39002CEF5C02F776E862D86C24D27448C429C6B176D2EC68CBAD C0
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="874183" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (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:	8e3536005799 59f0507d00376d2e56e8c9a24648b2574e e72fa81dec5d70874a
SHA512:	d492b9ea094bd6e695a562a855587feaf793be0cb35cf28 df681a0022a8e0139a222a68bd578fb65b125fe9fea86f1f 596bf337e65a445e8a5286d95ae037857
SSDEEP:	3072:U+NvJwwbI7mZgauugh+KsvkfGDLNj58E2wL6uE XKlwjwxhfgtRlh:9swbYmZgarrKsvVDR5POuE6lwqf4
File Content Preview:	MZ.....@.....!..L.!Th is 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 00007F7478743040h
cmp dword ptr [004550A0h], ebx
jne 00007F747876CACEh
push 0043E948h
call dword ptr [0044475Ch]
pop ecx
call 00007F747876CBC5h

Instruction
push 00453078h
push 00453074h
call 00007F747876CBB0h
mov eax, dword ptr [00455BF0h]
mov dword ptr [ebp-6Ch], eax
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 00007F747876CB7Dh

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	

DLL	Import
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
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 17:32:52.835212946 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:52.892349958 CET	53	65298	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:53.247808933 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:53.310240030 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:53.459800005 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:53.501657009 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:53.511421919 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:53.550204992 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:53.868103981 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:53.931855917 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:54.423717022 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:54.475142956 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:56.360182047 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:56.408806086 CET	53	49257	8.8.8.8	192.168.2.4

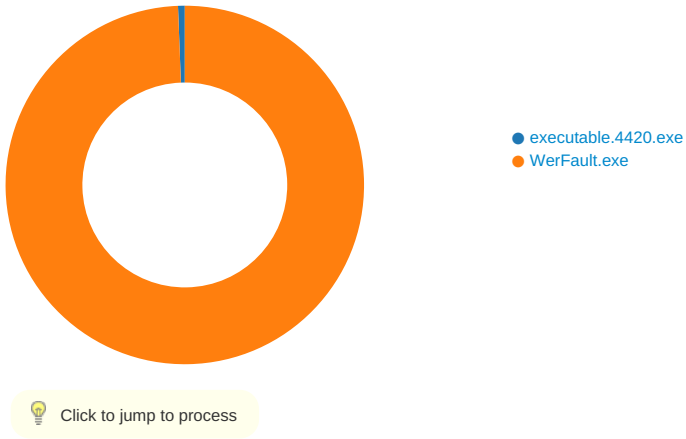
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:32:57.325617075 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:57.378972054 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:58.483364105 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:58.540673971 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 17:32:59.432522058 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:32:59.494601011 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:00.290999889 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:00.342525005 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:01.303342104 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:01.352052927 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:02.506978035 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:02.557471037 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:03.713850975 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:03.775391102 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:04.744421959 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:04.797744036 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:05.863677979 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:05.912419081 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:06.794970989 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:06.843676090 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:10.461750031 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:10.513417959 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:16.179717064 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:16.230974913 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:17.899775982 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:17.948786020 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:19.083235025 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:19.136178017 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:20.078944921 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:20.127528906 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:20.877273083 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:20.926132917 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:23.138626099 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:23.190361977 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:41.258702993 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:41.352114916 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:42.016740084 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:42.092366934 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:42.684490919 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:42.741871119 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:43.155957937 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:43.216820955 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:43.228245020 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:43.279541016 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:43.878380060 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:43.935725927 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:44.499895096 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:44.557358980 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:45.146218061 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:45.236953974 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:46.009835958 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:46.068258047 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:47.718394041 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:47.776036024 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:48.074347019 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:48.138317108 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:48.232470036 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:48.281176090 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:48.281677008 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:48.330260992 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:58.637748957 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:58.700093985 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 17:33:58.980968952 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:33:59.045989037 CET	53	59794	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:34:03.480015993 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:34:03.543883085 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 17:34:32.999061108 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:34:33.050477982 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 17:34:34.592492104 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 17:34:34.650958061 CET	53	60542	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: executable.4420.exe PID: 7112 Parent PID: 5900

General

Start time:	17:33:00
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	3C 2E 35 60 05 00 00 00	success or wait	1	41B11F	RegSetValueExA

Analysis Process: WerFault.exe PID: 5856 Parent PID: 7112

General

Start time:	17:33:02
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664
Imagebase:	0x3c0000
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	6E8F1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_1685813a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_1685813a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E8E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.tmp	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	success or wait	1	6E8E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	success or wait	1	6E8E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.tmp.xml	success or wait	1	6E8E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64AA.tmp.csv	success or wait	1	6E8E4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER67C8.tmp.txt	success or wait	1	6E8E4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 41 2e 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....A.5`.....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.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 0c 1c 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 c8 1b 00 00 3c 2e 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 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U.....B..... ..GenuineIntelW.....T... ....<.5`..... .....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 dd 12 77 27 1e 44 00 00 00 00 00 a0 14 0a 00 27 1e 44 00 23 00 00 00 46 02 01 00 80 14 0a 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...............p..w'.D..... ....'.D.#...F.......+.........	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	168	cc 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 27 1e 44 00 00 00 00 00 02 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 e6 20 00 00	........................'.D...	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	20	16 00 00 00 69 00 73 00 00 00 00 00 04 00 00 00 46 30 00 00	....i.s.........F0..	success or wait	22	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	4	00 c7 1e 74	...t	success or wait	21	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	524288	00 00 00 00 52 dd 12 77 80 15 0a 00 a8 fe 19 00 d0 15 0a 00 08 15 0a 00 04 21 0a 00 70 dd 12 77 a8 fe 19 00 68 15 0a 00 24 dd 12 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 11 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 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 00 00 00 00 a8 fe 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 10 21 0a 00 b6 b9 11 77 80 15 0a 00 d0 15 0a 00 80 15 0a	....R..w................!..p. .w....h...$..w............... '.D.............".w.......... ......'.D.................... ....!.. ...w...........	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	572	bc b1 11 77 d6 c9 0f 77 b0 00 00 00 aa aa aa aa 10 00 00 00 58 fe a5 00 24 ff a5 00 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 50 32 00 00 50 32 00 00 00 00 00 b0 00 00 00 aa aa aa aa b0 00 00 00 aa aa aa aa 00 50 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 70 4d 5a 00 00 00 00 00 00 00 00 00 18 6a 59 00 00 90 31 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 92 31 00 90 fe 95 00 88 6e 59 00 98 fe 95 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w...........X...$..... ..@..w@..w.....P2..P2......... ....P2.............. ....pMZ... ....jY...1................ ....T.1... ...nY........................	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 dd 12 77 27 1e 44 00 00 00 00 00 a0 14 0a 00 27 1e 44 00 23 00 00 00 46 02 01 00 80 14 0a 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...............p..w'.D..... ....'.D.#...F.......+.........	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	48	e4 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 32 00 00 00 00 00 c4 fd a5 00 00 00 00 00 3c 02 00 00 06 67 10 00 cc 02 00 00 16 2c 00 00	....P2............ <....g.......,..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	4	2a 00 00 00	*...	success or wait	42	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	44	26 00 00 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 00 00	&...e.x.e.c.u.t.a.b.l.e...4.4.2.0...e.x.e...	success or wait	42	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	752	00 00 60 76 00 00 00 00 00 60 00 00 f9 0a 01 00 51 32 d9 44 ce 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 04 00 00 00 00 e0 b3 02 00 00 00 00 00 00 20 03 00 00 00 00 06 54 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 af 76 03 00 00 00 00 00 03 77 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 24 1b 00 00 00 00 00 08 db 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 35 f1 04 00 00 00 00	..`v.....`......Q2.D. ....B.....B?..... ...."..... ..@E.....Zb..... .... .T.....v.....w .....8$..... @.....5.....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.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	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5865.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 bc 11 00 00 cc 07 00 00 05 00 00 00 64 01 00 00 e2 2e 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 5e 75 10 00 15 00 00 00 ec 01 00 00 88 19 00 00 16 00 00 00 98 00 00 00 74 1b 00 00	....T.....@...^u..... .....t...	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.1.2.<./.P.i.d.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.1.9.3.<./.U.p.t.i.m.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 39 00 35 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.7.9.5.5.8.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 39 00 35 00 31 00 37 00 34 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.>.9.7.9.5.1.7.4.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 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.>.2.5.7.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 38 00 31 00 39 00 35 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.>.9.9.8.1.9.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 38 00 31 00 39 00 35 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.>.9.9.8.1.9.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 32 00 31 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.>.3.2.1.0.4.<./.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.9.6.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 33 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.7.3.6.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 37 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.7.7.7.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 33 00 36 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.7.3.6.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 34 00 33 00 34 00 39 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.>.6.6.4.3.4.9.0.<./.U.p.t.i.m.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 36 00 35 00 31 00 33 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.>.4.6.5.1.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 36 00 33 00 37 00 37 00 32 00 31 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.>.1.0.6.3.7.7.2.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 30 00 30 00 32 00 34 00 35 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.0.2.4.5.5.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 37 00 34 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.9.7.4.5.4.4.<./.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 33 00 35 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.5.8.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 34 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.7.9.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 32 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.7.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 32 00 39 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.2.9.8.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 38 00 31 00 31 00 37 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.1.1.7.3.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 32 00 39 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.2.9.8.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 73 00 63 00 72 00 62 00 6f 00 67 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.>.s.c.r.b.o.g.,. .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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 73 00 63 00 72 00 62 00 6f 00 67 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.>.s.c.r.b.o.g.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 39 00 38 00 31 00 34 00 38 00 33 00 31 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.9.8.1.4.8.3.1.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 33 00 54 00 31 00 36 00 3a 00 33 00 33 00 3a 00 30 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.6.:.3.3.:.0.7.Z.".>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 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 36 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.2.". .P.I.D.=.".7.1.1.2.". .U.p.t.i.m.e.M.S.=.".6.5.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".6.5.6.". .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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 33 00 38 00 66 00 30 00 34 00 36 00 30 00 2d 00 33 00 35 00 38 00 33 00 2d 00 34 00 62 00 33 00 37 00 2d 00 39 00 66 00 33 00 39 00 2d 00 38 00 36 00 33 00 34 00 62 00 36 00 32 00 38 00 63 00 33 00 64 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.3.8.f.0.4.6.0.-.3.5.8.3.-.4.b.3.7.-.9.f.3.9.-.8.6.3.4.b.6.2.8.c.3.d.0.<./.G.u.i.d.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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 33 00 54 00 31 00 36 00 3a 00 33 00 33 00 3a 00 30 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.6.:.3.3.:.0.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER62F5.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	6E8E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64BB.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	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_1685813a\Report.wer	unknown	2	ff fe	..	success or wait	1	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_1685813a\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	172	6E8E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_executable.4420._c4d235e04f7d67dd8b9808a243ef65182404b_dc10a768_1685813a\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 39 00 35 00 37 00 31 00 36 00 35 00 37 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.6.9.5.7.1.6.5.7.5.	success or wait	1	6E8E497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	success or wait	1	6E9036BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E901FB2	RegCreateKeyExW
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E8E43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	ProgramId	unicode	000677be299c7994b95377cd62c15c1999190000ffff	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	FileId	unicode	0000166886066ffabb76f6b72c4b4ed91fa19e59987a	success or wait	1	6E9036BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	LowerCaseLongPath	unicode	c:\users\user\desktop\executable.4420.exe	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	LongPathHash	unicode	executable.4420.|17812628	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	Name	unicode	executable.4420.exe	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	Publisher	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	Version	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	BinFileVersion	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	BinaryType	unicode	pe32_i386	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	ProductName	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	ProductVersion	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	LinkDate	unicode	11/01/2007 08:49:26	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	BinProductVersion	unicode		success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	Size	B	00 B0 06 00 00 00 00 00	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	Language	dword	0	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	IsPeFile	dword	1	success or wait	1	6E9036BF	unknown
\REGISTRY\A\{5b95e138-7231-9eea-bbe4-7a96c5231493}\Root\InventoryApplicationFile\executable.4420.|17812628	IsOsComponent	dword	0	success or wait	1	6E9036BF	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E901FE8	RegSetValueExW

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

Disassembly

Code Analysis