ID: 247352
Sample Name: zeus 1_1.3.3.6.vir
Cookbook: default.jbs
Time: 03:50:54
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

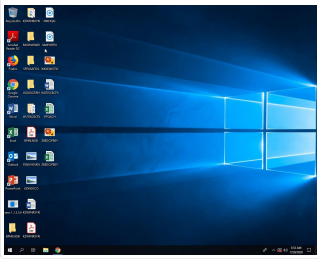
Analysis Report zeus 1_1.3.3.6.vir

Overview

General Information

Sample Name:	zeus 1_1.3.3.6.vir (renamed file extension from vir to exe)
Analysis ID:	247352
MD5:	37b593c8e58ab5..
SHA1:	9b8895a9461fcfd..
SHA256:	baa8f2980a3a3a9.

Most interesting Screenshot:



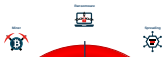
Detection

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…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…
- Contains functionality to call native f…
- Creates files inside the system direc…
- Enables debug privileges
- One or more processes crash
- Queries disk information (often used…
- Sample execution stops while proce…
- Sample file is different than original …
- Stores large binary data to the regist…

Classification



Startup

- **System is w10x64**
- zeus 1_1.3.3.6.exe (PID: 4700 cmdline: 'C:\Users\user\Desktop\zeus 1_1.3.3.6.exe' MD5: 37B593C8E58AB5A3A10C0FF8918DC92F)
  - WerFault.exe (PID: 4988 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4700 -s 368 MD5: 80E91E3C0F5563E4049B62FCAF5D67AC)
- **cleanup**

Malware Configuration

No configs have been found

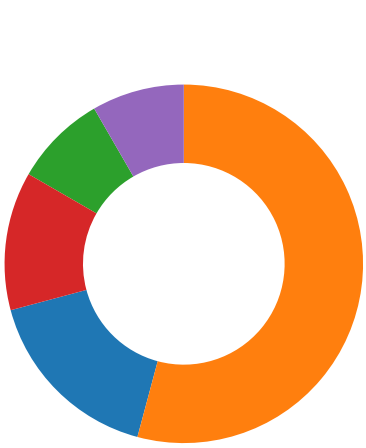
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

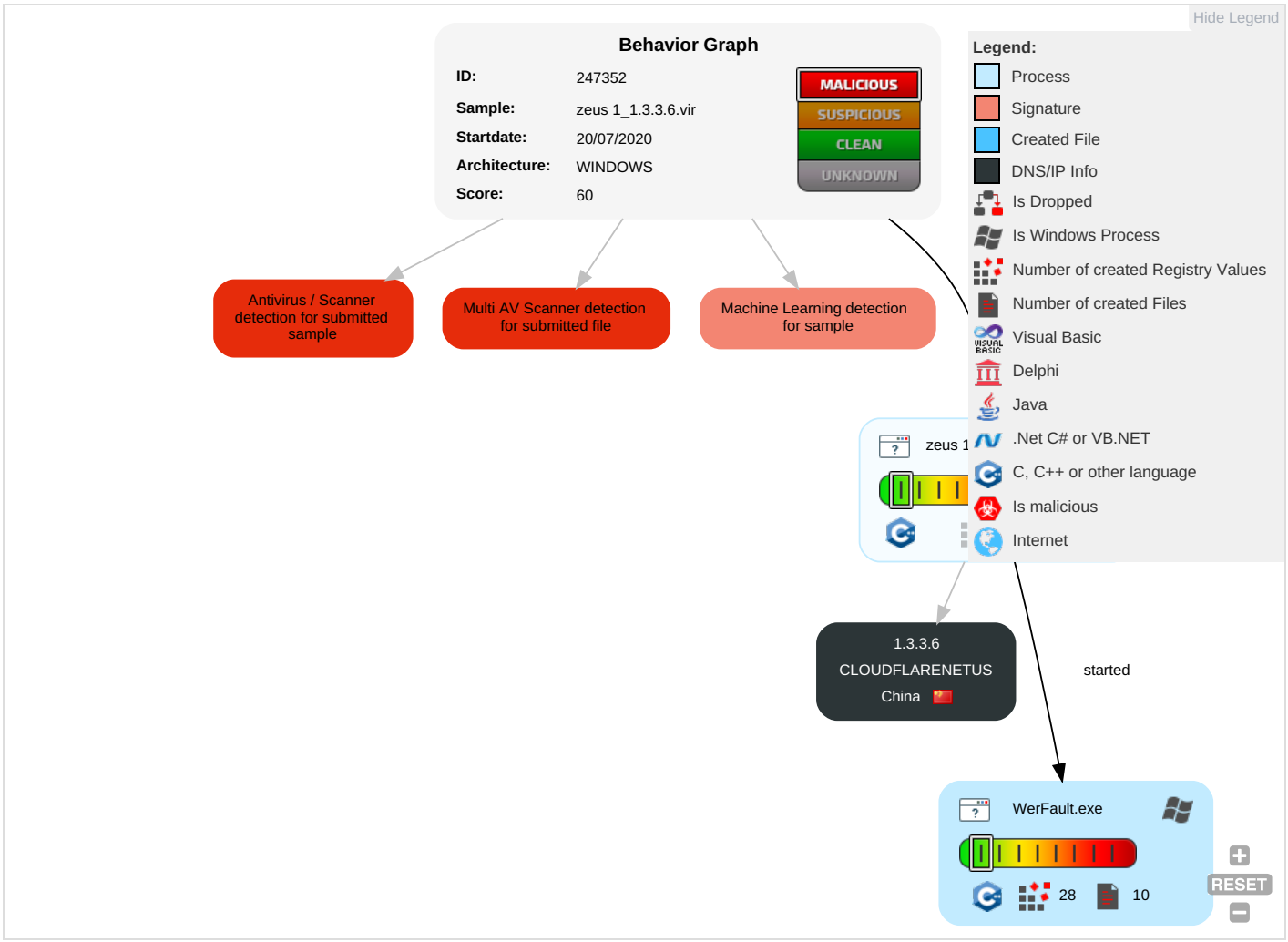
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Remote Management	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	Virtualization/Sandbox Evasion 2	Application Deployment Software	Data from Local System	Data Compressed	Data Obfuscation	Eavesdrop Insecure Network Communica
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Software Packing 1	Network Sniffing	Process Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS7 Redirect Ph Calls/SMS
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Modify Registry 1	Input Capture	Security Software Discovery 2	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 Track Devic Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Virtualization/Sandbox Evasion 2	Credentials in Files	System Information Discovery 1 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Process Injection 1	Account Manipulation	Remote System Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communica
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	DLL Side-Loading 1	Brute Force	System Owner/User Discovery	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jamming o Denial of Service

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
zeus 1_1.3.3.6.exe	83%	Virustotal		Browse
zeus 1_1.3.3.6.exe	67%	Metadefender		Browse
zeus 1_1.3.3.6.exe	93%	ReversingLabs	Win32.Trojan.Zbot	
zeus 1_1.3.3.6.exe	100%	Avira	TR/Dropper.Gen	
zeus 1_1.3.3.6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.zeus 1_1.3.3.6.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.zeus 1_1.3.3.6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.zeus 1_1.3.3.6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

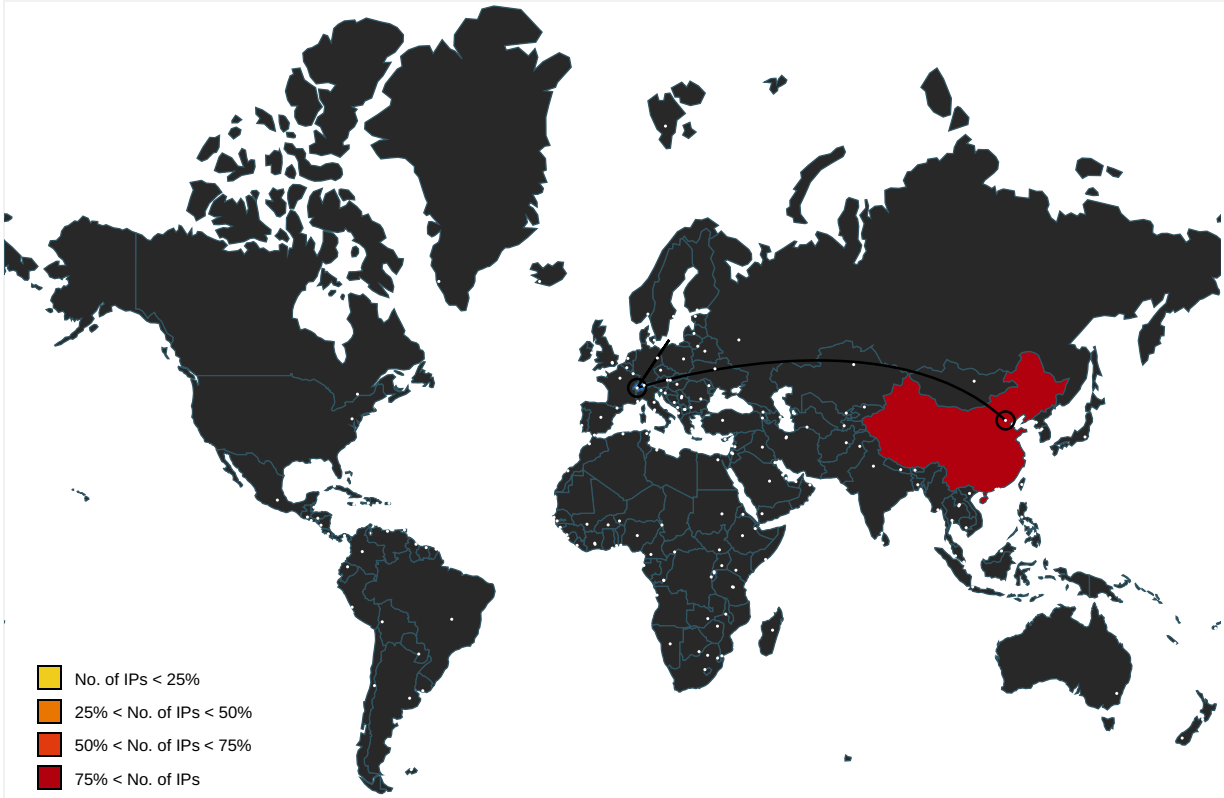
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.3.3.6	China		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247352
Start date:	20.07.2020
Start time:	03:50:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeus 1_1.3.3.6.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	7
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@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.4% (good quality ratio 72.4%) • Quality average: 53.9% • Quality standard deviation: 38.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.90.137.126, 40.90.23.247, 40.90.137.124, 40.90.137.120, 40.90.23.208, 40.90.23.153, 40.90.137.125, 40.90.23.206, 51.143.111.7, 2.18.68.82 • Excluded domains from analysis (whitelisted): umwatson.trafficmanager.net, fs.microsoft.com, login.live.com, www.tm.lg.prod.aadmsa.akadns.net, e1723.g.akamaiedge.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, login.msa.msidentity.com

Simulations

Behavior and APIs

Time	Type	Description
03:51:30	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://comtechadsl.com/ehepsqm.exe	Get hash	malicious	Browse	• 104.20.74.28
	http://blueeyeswebsite.com/	Get hash	malicious	Browse	• 104.24.110.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT20893.HTML	Get hash	malicious	Browse	• 104.16.133.229
	ATT84128.HTML	Get hash	malicious	Browse	• 104.16.133.229
	http://https://bit.ly/30cSl6K	Get hash	malicious	Browse	• 104.16.124.96
	http://https://jhmetalinc-my.sharepoint.com/:o:/p/office/EiJ0PCnWDtJHiWQIXRi7bWgB6cFzFQtLhcLET3v8d3NRLA?rtime=ORiHa4Eq2Eg	Get hash	malicious	Browse	• 104.16.132.229
	ATT39268.HTM	Get hash	malicious	Browse	• 104.16.133.229
	payment730.xls	Get hash	malicious	Browse	• 104.27.180.83
	http://atcsagacity.com/wp-admin/MYWZIKG/eigyho/s9w08163326462037l3g44z0n2u/	Get hash	malicious	Browse	• 172.67.186.191
	http://https://gogoanime1.net/.well-known/acme-challenge/bid/login.php	Get hash	malicious	Browse	• 104.16.132.229
	http://https://lroetrgpfxciziew.frb.io/?bbre=pdsi93reodfxci	Get hash	malicious	Browse	• 104.16.133.229
	http://mapfrecomercial.com/	Get hash	malicious	Browse	• 104.16.202.237
	http://https://event.on24.com/wcc/r/2462461/BB0A869CCD07459AE0E4C73F0AD810E3/1209023?partnerref=connect	Get hash	malicious	Browse	• 104.17.71.206
	http://https://u10500736.ct.sendgrid.net/ls/click?upn=GJ-2Fwg0v0GjXICnjOzCZwjhkRw9-2BbFlj0p-2BETjV5NQUzZanQeaYMDpzIDJ401Kach0E7l_YxCxpoge33FNHhRVcK23d3jJCq3cIHwc-2BD1XeO3y4vWhDSyEnUs6U-2FsQ3r28LvMmBf0-2FyPTfw7LkuX8KPrqtuiBKVLJGudFG5cgos-2FYMheOpZ3KzgDMXMKE-2BA6yiT-2Bi5BQtK80dm1zrijWZnCRa6hF0zjqp3QnkLp0NHHccLK9ZW3lYLn1ntwPI5yxeaqK-2FwMj6c4bzGzF8lmQMxhNRSLY2oartjGJW1716gR3wWT6FnAMuuMr-2BmVOWIDO3doJzx	Get hash	malicious	Browse	• 104.22.0.232
	http://youbue.com	Get hash	malicious	Browse	• 104.20.21.239
	MuMuInstaller_1.1.0.4_a2ca17_yxmrfz_zh-Hans_1573441614.exe	Get hash	malicious	Browse	• 1.1.0.4
	Invoice2867.hTMl	Get hash	malicious	Browse	• 104.27.165.84
	http://https://www.seat26.com/wp-includes/js/tinymce/plugins/colorpicker/gastblogg/warenkorb.php?street=kqh1sdty120gb0c&face=guess&window=section	Get hash	malicious	Browse	• 104.16.132.229
	http://www.hobbyfarms.com/how-to-build-a-vermin-proof-chicken-feeder/	Get hash	malicious	Browse	• 104.18.99.60
	Scanned_from_Xerox_Multifunction.htm	Get hash	malicious	Browse	• 104.16.133.229

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus 1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Size (bytes):	9346
Entropy (8bit):	3.7743698682666538
Encrypted:	false
MD5:	CA60C35214E062F83B062EB2E3EA0F5D
SHA1:	39289783C2640E2C8EF8BF7F1001B28FF9A90B18
SHA-256:	60F34D46582E4BA9BF0412470A65AC7E691484199DC26551AAD3CCEE0E342158
SHA-512:	13C127A8613035A1E31D1D2315F6BB8066E7334D764CDAB5B54FABB3B0A2514A7FC1F1DCA49BABC42CF32F9819B4C2410F7740555F1E2EA831FB8932C86009F
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus 1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_13400 24e\Report.wer	
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.=.1.3.2.3.9.7.1.5.8.8.8.2.7.3.1.6.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.3.9.7.1.5.8.8.8.8.1.3.7.0.1.4.....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.=.c.1.0.f.a.d.9.5.-.5.f.8.1.-.4.7.4.2.-.a.5.2.d.-.e.8.5.8.c.0.2.6.d.9.5.c.....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.=.9.0.f.2.2.9.3.8.-.7.6.9.6.-.4.f.3.c.-.9.f.7.3.-.b.e.e.0.a.5.6.9.9.4.6.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.z.e.u.s. .1._.1...3...3...6...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.5.c.-.0.0.0.1.-.0.0.2.3.-.b.f.2.c.-.e.4.b.6.8.3.5.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.a.7.1.5.b.5.9.9.b.b.1.8.7.8.e.b.2.e.0.2.a.9.5.1.6.c.1.9.7.a.d.0.0.0.0.0.8.0.0.!.0.0.0.0.9.b.8.8.9.5.a.9.4.6.1.f.c.f.d.6.3.6.5.3.6.4.1.7.f.0.5.6.4.b.2.e.a.0.2.5.6.8.a.6.!.z.e.u.s. .1._.1...3...3...6...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Jul 20 10:51:28 2020, 0x1205a4 type
Size (bytes):	32208
Entropy (8bit):	2.0347463611275103
Encrypted:	false
MD5:	C2404B26466B85CE314DD8871EECB2E4
SHA1:	73E6D51AF744CD17D18AFF63146E8D7FBC48332B
SHA-256:	471926DB60321580DA52B55510F7B1B6A6CCB060D91F3FDF3846ACC8EC3E44E3
SHA-512:	E70044C521A5D72F377A29B11FEE3E7FBF1243A776D122AF83B0D9ABEE3BC2636EBFCCB3BA6A86EF1702A198FFEC0937F82F33E16E00FB4B6EB6C5FB05861F35
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....0w._.....?.....B.....GenuineIntel.....T.....\...-w._.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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
Size (bytes):	8298
Entropy (8bit):	3.6972257005162006
Encrypted:	false
MD5:	329BF45F15F3D8D0CC5F20DE54957CAE
SHA1:	E30474E9CF52B6294D04B5B1DFFB322239011351
SHA-256:	9958448211381454823EE17937526B1D61042D27D863C81973FF0635A18BCB3C
SHA-512:	642376370C0DAEACD4FD6F1697F2BD984AE661F389B04F926DBE22C81AF07E398948C9EB4E467325FFA2598691F795D4ED55AA20877F0F73CBBF2D5E97D9F28
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...1.6.5...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.>.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.7.0.0.<./.P.i.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Size (bytes):	4555
Entropy (8bit):	4.471367933113011
Encrypted:	false
MD5:	94416F3B84D01F864BD26EE8EF7338B0
SHA1:	EABD5819BD737447CDF53E926532DEBD3C50AD42
SHA-256:	34263F4840EE41D2EEA4F4F1D446ABA80C28DC6C87A5AD2D7828CC3FC3C973D1
SHA-512:	12C207BB4D5A01DB43553AEC2FD980E9138BBF92A060F77AE32FB98207868C5914A2221C1B4C4CE1BA7C6D2079D1FA156CD2AFBECE40CCA68908A522F286D5E8
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="165" />.. <arg nm="verqfe" val="165" />.. <arg nm="csdbld" val="165" />.. <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="1064268" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.165.17134.0-11.0.75" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="2048" /

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.532649763156255
TrID:	• Win32 Executable (generic) a (10002005/4) 99.92% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	zeus 1_1.3.3.6.exe
File size:	203264
MD5:	37b593c8e58ab5a3a10c0ff8918dc92f
SHA1:	9b8895a9461fcfd636536417f0564b2ea02568a6
SHA256:	baa8f2980a3a3a98c8841ebbdedde17688cc1464094d02c9c1e4b3bcda950438
SHA512:	e823696571303aaac73f5604a2d89f406b9fc1a7c13fff1fb40f19805ad84b68489307da39023f7c43fc4a68f7ecb54da5ad3a5bae3b1643fc466352c44acfe3
SSDEEP:	3072:rMq0cmnRvfXQRu/2lUQYyrWpWxQGrZqxg7FXfCuXqAc60ynh0WczECh:rMDcwRnOl/2W2Gr0qguv0ynQE
File Content Preview:	MZ.....@..... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401439
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:	0x41F82662 [Wed Jan 26 23:23:14 2005 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	9
OS Version Minor:	4
File Version Major:	9
File Version Minor:	4
Subsystem Version Major:	9
Subsystem Version Minor:	4
Import Hash:	903bbbc1e30a3ce0c17dab78d9ae9b8b

Entrypoint Preview

Instruction
cmp dword ptr [ebp-10h], 00000000h
jne 00007F435CCCCD00h
sbb eax, 00004946h
or esi, 004A434Fh
jmp 00007F435CCCCD70h
cmp edx, 6E374551h
je 00007F435CCCCCF4h
jmp 00007F435CCCCD66h
test dword ptr [ebp-1Ch], 00000004h

Instruction
jne 00007F435CCCCD0Eh
push 00004C36h
lea edx, dword ptr [ebp-00000170h]
push edx
push dword ptr [ebp-30h]
push dword ptr [ebp-00000124h]
call 00007F435CCCCC8Ah
jmp 00007F435CCCCD41h
test esi, 00020000h
jne 00007F435CCCCD03h
push dword ptr [ebp-00000114h]
push dword ptr [ebp-14h]
push edx
call 00007F435CCCD2B9h
jmp 00007F435CCCCD28h
test dword ptr [ebp-2Ch], 04000000h
jne 00007F435CCCCD03h
lea edx, dword ptr [ebp-000000ECh]
push edx
call 00007F435CCCD170h
jmp 00007F435CCCCD11h
test dword ptr [ebp-2Ch], 00001000h
je 00007F435CCCCCFBh
jmp 00007F435CCCCCFFh
cmp dword ptr [ebp-2Ch], 00000000h
jne 00007F435CCCCCF6h
mov esi, 00007154h
sbb edi, 00006672h
adc ebx, 44h
xor edx, 00006131h
push ebp
mov ebp, esp
add esp, FFFFFF7Ch
cmp edi, 79h
je 00007F435CCCCD05h
sbb dword ptr [ebp-10h], esi
mov dword ptr [ebp-08h], ebx
sbb dword ptr [ebp-24h], 00000000h
jmp 00007F435CCCC880h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7078	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x33000	0x38c	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6000	0x6000	False	0.510091145833	data	4.98789507629	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1000	0x400	False	0.345703125	data	3.08620186062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x8000	0x2b000	0x2ae00	False	0.862148095845	data	6.52478510037	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x33000	0x27000	0x400	False	0.484375	data	3.65152224082	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x33058	0x334	data	Russian	Russia

Imports

DLL	Import
KERNEL32.DLL	GetTickCount, GetModuleFileNameA, SleepEx, GetCurrentThreadId, FormatMessageW, SetEvent, GetModuleHandleA, GetCommandLineA, VirtualAllocEx, CreateEventA
GDI32.DLL	SelectObject, GetObjectW, DeleteObject, DeleteDC, MoveToEx, DeleteObject, GetDeviceCaps, SetTextColor, SelectObject
USER32.DLL	GetSystemMetrics, ShowWindow, DefWindowProcW, GetDC, LockWindowStation, CreateWindowExW, GetWindowRect

Version Infos

Description	Data
LegalCopyright	
InternalName	
FileVersion	58.90.79.59
CompanyName	
ProductName	
ProductVersion	58.90.79.59
FileDescription	
OriginalFilename	WsO.exe
Translation	0x0008 0x0000

Possible Origin

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

Network Behavior

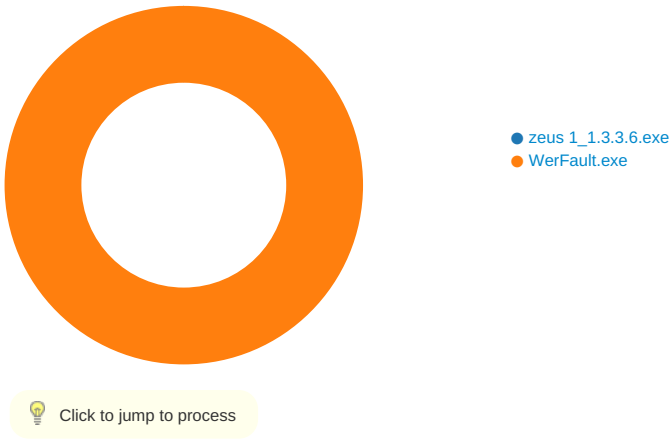
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2020 03:51:29.422877073 CEST	56689	53	192.168.2.7	8.8.8.8
Jul 20, 2020 03:51:29.456759930 CEST	53	56689	8.8.8.8	192.168.2.7
Jul 20, 2020 03:51:30.063621044 CEST	64966	53	192.168.2.7	8.8.8.8
Jul 20, 2020 03:51:30.089025974 CEST	53	64966	8.8.8.8	192.168.2.7
Jul 20, 2020 03:51:38.702860117 CEST	56768	53	192.168.2.7	8.8.8.8
Jul 20, 2020 03:51:38.736690044 CEST	53	56768	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: zeus 1_1.3.3.6.exe PID: 4700 Parent PID: 4884

General

Start time:	03:51:25
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeus 1_1.3.3.6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeus 1_1.3.3.6.exe'
Imagebase:	0x400000
File size:	203264 bytes
MD5 hash:	37B593C8E58AB5A3A10C0FF8918DC92F
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 4988 Parent PID: 4700

General

Start time:	03:51:27
Start date:	20/07/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4700 -s 368
Imagebase:	0x1130000
File size:	434584 bytes
MD5 hash:	80E91E3C0F5563E4049B62FCAF5D67AC
Has administrator privileges:	false
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	70BB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70BA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	success or wait	1	70BA4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	success or wait	1	70BA4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp.xml	success or wait	1	70BA4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C7.tmp.csv	success or wait	1	70BA4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5D7.tmp.txt	success or wait	1	70BA4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 30 77 15 5f a4 05 12 00 00 00 00 00	MDMP..... .....0w._.....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	1420	00 00 06 00 02 3f 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 94 12 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c f2 06 03 00 ff fb 8b 17 00 00 00 00 54 05 00 00 f7 03 00 00 5c 12 00 00 2d 77 15 5f 00 00 00 00 00 00 00 00 a4 0d 00 00 a4 0d 00 00 a4 0d 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....?...........B............ ..GenuineIntel............T... ....\...-w._.................. ....0..2.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 c0 52 00 00 5a 51 58 00 21 0a 25 af 00 00 00 00 9a 19 51 1e 00 00 00 00 94 ff 19 00 a0 59 40 00 23 00 00 00 46 02 01 00 80 ff 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+....R..ZQX.!.%.......Q..... .....Y@.#...F.......+.........	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	168	28 05 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 a0 59 40 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9a 19 51 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ec 14 00 00	(........................Y@... ....Q.........	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	20	0e 00 00 00 20 59 40 00 00 00 00 00 00 01 00 00 00 21 00 00	.... Y@..........!..	success or wait	14	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	256	00 83 f0 61 c9 c2 10 00 53 e8 b2 fd ff ff e8 b3 fd ff ff 8d 8d 68 fe ff ff 51 8d 55 a4 52 68 6a 56 00 00 50 e8 bb ff ff ff e8 44 05 00 00 8d 8d 48 ff ff ff 51 8d 4d 84 51 68 aa 3a a7 92 e8 c4 fd ff ff 53 68 37 4a 00 00 ff b5 b0 fe ff ff 6a 4c e8 92 04 00 00 52 ff b5 d0 fe ff ff ff b5 28 ff ff ff 68 b3 d0 3e f1 e8 5f fd ff ff e8 2f 06 00 00 e8 b7 01 00 00 6a 00 6a 01 e8 58 fd ff ff 0f b7 01 3d c2 08 00 00 74 01 c3 6a 6d 68 41 62 00 00 6a 69 68 36 b3 63 8d e8 2d 00 00 00 e9 d0 01 00 00 24 21 10 24 24 84 24 21 01 00 01 24 84 01 21 24 84 24 01 01 21 01 21 84 10 01 84 21 84 24 10 01 00 24 84 01 10 24 21 24 ff 25 3c 70 40 00 01 5d f4 09 75 94 81 9d 40 ff ff ff 38 50 64 00 83 75 c4 73 f7 55 b4 f7 55 a8 81 a5 74 ff ff ff 76 75 46 69 11 5d b8 ff 45 a8 f7 5d 88 f7	...a....S............h...Q.U.R hjV..P......D.....H...Q.M.Qh. :.......Sh7J........jL.....R........ (...h..>.._..../........j .j..X......=....t..jmhAb..jih6 .c..-........$!.$$.$!...$..!$. $..!.!....!.$...$...$!$.%<p@..]..u...@...8Pd..u.s.U..U...t.. .vuFi.]..E..]..	success or wait	13	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	2492	bc a7 19 77 23 1f e1 73 aa aa aa aa 78 f8 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 6c 01 00 00 68 01 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 40 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 78 f8 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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#..s....x................ ......l...h.......$........... ....@- ....x..............	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 d8 f7 19 00 bc a7 19 77 23 00 00 00 06 02 00 00 48 f6 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#.......H...+.........	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	48	b4 03 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 d0 2d 00 00 00 00 00 c4 fd 8b 00 00 00 00 00 3c 02 00 00 e4 5a 00 00 cc 02 00 00 50 1d 00 00	....-............. <....Z......P...	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	4	14 00 00 00	....	success or wait	20	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	42	24 00 00 00 7a 00 65 00 75 00 73 00 20 00 31 00 5f 00 31 00 2e 00 33 00 2e 00 33 00 2e 00 36 00 2e 00 65 00 78 00 65 00 00 00	$...z.e.u.s. .1._.1...3...3...6...e.x.e...	success or wait	20	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	752	00 00 bd 73 00 00 00 00 00 40 04 00 12 36 04 00 9b c6 fc 0b d0 14 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 8d ff 07 00 01 00 00 00 ef ff 07 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 80 a3 01 00 00 00 00 00 c0 58 02 00 00 00 00 be 87 02 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 0b 38 03 00 00 00 00 00 08 80 03 00 00 00 00 00 4e 5a 00 00 00 00 00 00 00 57 46 1a 00 00 00 00 00 e9 b8 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 34 c6 05 00 00 00 00	...s.....@...6.....B.....B?.....$.....@A.....Zb.....X.....8.....NZ.....WF.....@.....4.....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	5948	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	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF85B.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 74 08 00 00 9c 07 00 00 05 00 00 00 e4 00 00 00 1c 20 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 e8 0e 00 00 30 6f 00 00 15 00 00 00 ec 01 00 00 10 10 00 00 16 00 00 00 98 00 00 00 fc 11 00 00	................t..... .....T.....8..... ....T.....0o.....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	138	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 36 00 35 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...1.6.5...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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	48	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 36 00 35 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.>.1.6.5.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.7.0.0.<./.P.i.d.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 7a 00 65 00 75 00 73 00 20 00 31 00 5f 00 31 00 2e 00 33 00 2e 00 33 00 2e 00 36 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.>.z.e.u.s. .1._.1...3...3...6...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 30 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.>.3.0.0.3.<./.U.p.t.i.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 35 00 31 00 30 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.2.5.1.0.7.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 31 00 32 00 36 00 39 00 36 00 33 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.1.2.6.9.6.3.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.4.4.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 35 00 34 00 38 00 30 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.4.8.0.4.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 35 00 34 00 38 00 30 00 34 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.4.8.0.4.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.8.8.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.7.2.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 31 00 34 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.1.4.5.6.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 31 00 34 00 32 00 38 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.>.1.4.2.8.8.<./.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 31 00 32 00 39 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.2.9.8.4.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 31 00 33 00 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.3.0.6.6.2.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 31 00 32 00 39 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.2.9.8.4.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 30 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.0.2.4.<./.P.i.d.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 34 00 34 00 31 00 32 00 32 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.4.4.1.2.2.4.<./.U.p.t.i.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 39 00 35 00 36 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.9.5.6.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 36 00 36 00 33 00 34 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.8.6.6.3.4.4.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 35 00 35 00 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.5.5.5.2.3.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 39 00 36 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.9.6.0.2.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 38 00 39 00 37 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.9.7.0.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.8.9.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.0.8.4.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 32 00 34 00 34 00 38 00 35 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.>.3.2.4.4.8.5.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 33 00 33 00 32 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.3.3.2.0.9.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 32 00 34 00 34 00 38 00 35 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.>.3.2.4.4.8.5.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 7a 00 65 00 75 00 73 00 20 00 31 00 5f 00 31 00 2e 00 33 00 2e 00 33 00 2e 00 36 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.>.z.e.u.s. .1._.1...3...3...6...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 45 00 33 00 38 00 42 00 36 00 30 00 42 00 33 00 2d 00 35 00 46 00 46 00 41 00 2d 00 34 00 46 00 38 00 38 00 2d 00 41 00 41 00 35 00 38 00 2d 00 43 00 44 00 44 00 34 00 39 00 37 00 45 00 37 00 43 00 42 00 32 00 32 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.E.3.8.B.6.0.B.3.-.5.F.F.A.-.4.F.8.8.-.A.A.5.8.-.C.D.D.4.9.7.E.7.C.B.2.2.<./.M.I.D.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 69 00 64 00 6e 00 62 00 69 00 6b 00 6c 00 20 00 47 00 6d 00 62 00 48 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.>.i.d.n.b.i.k.l. .G.m.b.H.<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	98	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 64 00 64 00 73 00 79 00 71 00 6c 00 79 00 66 00 65 00 66 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.>.d.d.s.y.q.l.y.f.e.f.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	74	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 64 00 64 00 73 00 79 00 71 00 6c 00 79 00 66 00 65 00 66 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.>.d.d.s.y.q.l.y.f.e.f.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 39 00 33 00 35 00 38 00 39 00 35 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.9.3.5.8.9.5.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 38 00 2d 00 30 00 37 00 2d 00 31 00 32 00 54 00 30 00 39 00 3a 00 30 00 32 00 3a 00 35 00 36 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.>.2.0.1.8.-.0.7.-.1.2.T.0.9.:.0.2.:.5.6.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	114	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 4e 00 6f 00 74 00 43 00 61 00 70 00 61 00 62 00 6c 00 65 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.>.N.o.t.C.a.p.a.b.l.e.<./.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 30 00 2d 00 30 00 37 00 2d 00 32 00 30 00 54 00 31 00 30 00 3a 00 35 00 31 00 3a 00 32 00 38 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.0.7.-.2.0.T.1.0.:.5.1.:.2.8.Z.".>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 37 00 30 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 37 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.4.". .P.I.D.=.".4.7.0.0.". .U.p.t.i.m.e.M.S.=.".3.7.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.7.7.". .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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 31 00 30 00 66 00 61 00 64 00 39 00 35 00 2d 00 35 00 66 00 38 00 31 00 2d 00 34 00 37 00 34 00 32 00 2d 00 61 00 35 00 32 00 64 00 2d 00 65 00 38 00 35 00 38 00 63 00 30 00 32 00 36 00 64 00 39 00 35 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.1.0.f.a.d.9.5.-.5.f.8.1.-.4.7.4.2.-.a.5.2.d.-.e.8.5.8.c.0.2.6.d.9.5.c.<./.G.u.i.d.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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 30 00 2d 00 30 00 37 00 2d 00 32 00 30 00 54 00 31 00 30 00 3a 00 35 00 31 00 3a 00 32 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.0.7.-.2.0.T.1.0.:.5.1.:.2.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9B3.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	70BA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA41.tmp.xml	unknown	4555	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	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus 1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e\Report.wer	unknown	2	ff fe	..	success or wait	1	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus 1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e\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	150	70BA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zeus 1_1.3.3.6.e_e4c97facf2e6c21ad4b59c1c4dfc8325877e68_c2261e74_1340024e\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 39 00 36 00 30 00 36 00 32 00 31 00 33 00 31 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.9.6.0.6.2.1.3.1.8.	success or wait	1	70BA497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	success or wait	1	70BC36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70BC1FB2	RegCreateKeyExW
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	70BA43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{39cab07b-c2a4-4ae8-888f-94b33c6c2c1a}	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	ProgramId	unicode	0006ba715b599bb1878eb2e02a9516c197ad00000800	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	FileId	unicode	00009b8895a9461fcfd636536417f0564b2ea02568a6	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	LowerCaseLongPath	unicode	c:\users\user\desktop\zeus 1_1.3.3.6.exe	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	LongPathHash	unicode	zeus 1_1.3.3.6.e|b989856c	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Name	unicode	zeus 1_1.3.3.6.exe	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Publisher	unicode		success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Version	unicode		success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	BinFileVersion	unicode	58.90.79.59	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	BinaryType	unicode	pe32_i386	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	ProductName	unicode		success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	ProductVersion	unicode		success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	LinkDate	unicode	01/26/2005 23:23:14	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	BinProductVersion	unicode	58.90.79.59	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Size	B	00 1A 03 00 00 00 00 00	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Language	dword	8	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	IsPeFile	dword	1	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	IsOsComponent	dword	0	success or wait	1	70BC36BF	unknown
\REGISTRY\A\{c959fbf4-3b0c-a87a-b0cf-d1fb805aedcc}\Root\InventoryApplicationFile\zeus 1_1.3.3.6.e|b989856c	Usn	B	70 0B A1 0A 00 00 00 00	success or wait	1	70BC36BF	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 A0 59 40 00 02 00 00 00 00 00 00 00 9A 19 51 1E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	70BC1FE8	RegSetValueExW

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

Disassembly

Code Analysis