ID: 231872
Sample Name: covid19.exe
Cookbook: default.jbs
Time: 19:10:54
Date: 20/05/2020
Version: 28.0.0 Lapis Lazuli

Table of Contents

Analysis Report covid19.exe

Overview

General Information

Sample Name:	covid19.exe
MD5:	d0a7273fc33b37a.
SHA1:	401279da57773a..
SHA256:	27725450780b19..

Most interesting Screenshot:

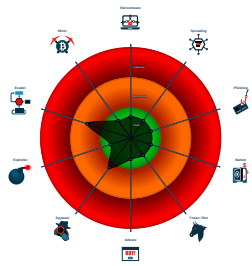
Detection

Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Checks if the current process is bein…
- Creates files inside the system direc…
- Enables debug privileges
- One or more processes crash
- PE file contains strange resources
- Queries disk information (often used …
- Queries the volume information (nam…
- Sample file is different than original f…
- Tries to load missing DLLs
- Uses code obfuscation techniques (c…

Classification



Startup

- **System is w10x64**
- covid19.exe (PID: 1096 cmdline: 'C:\Users\user\Desktop\covid19.exe' MD5: D0A7273FC33B37A38336213B86DEF543)
  - WerFault.exe (PID: 1624 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1096 -s 1040 MD5: 80E91E3C0F5563E4049B62FCAF5D67AC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

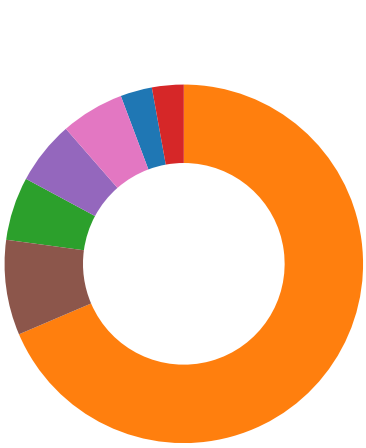
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Networking

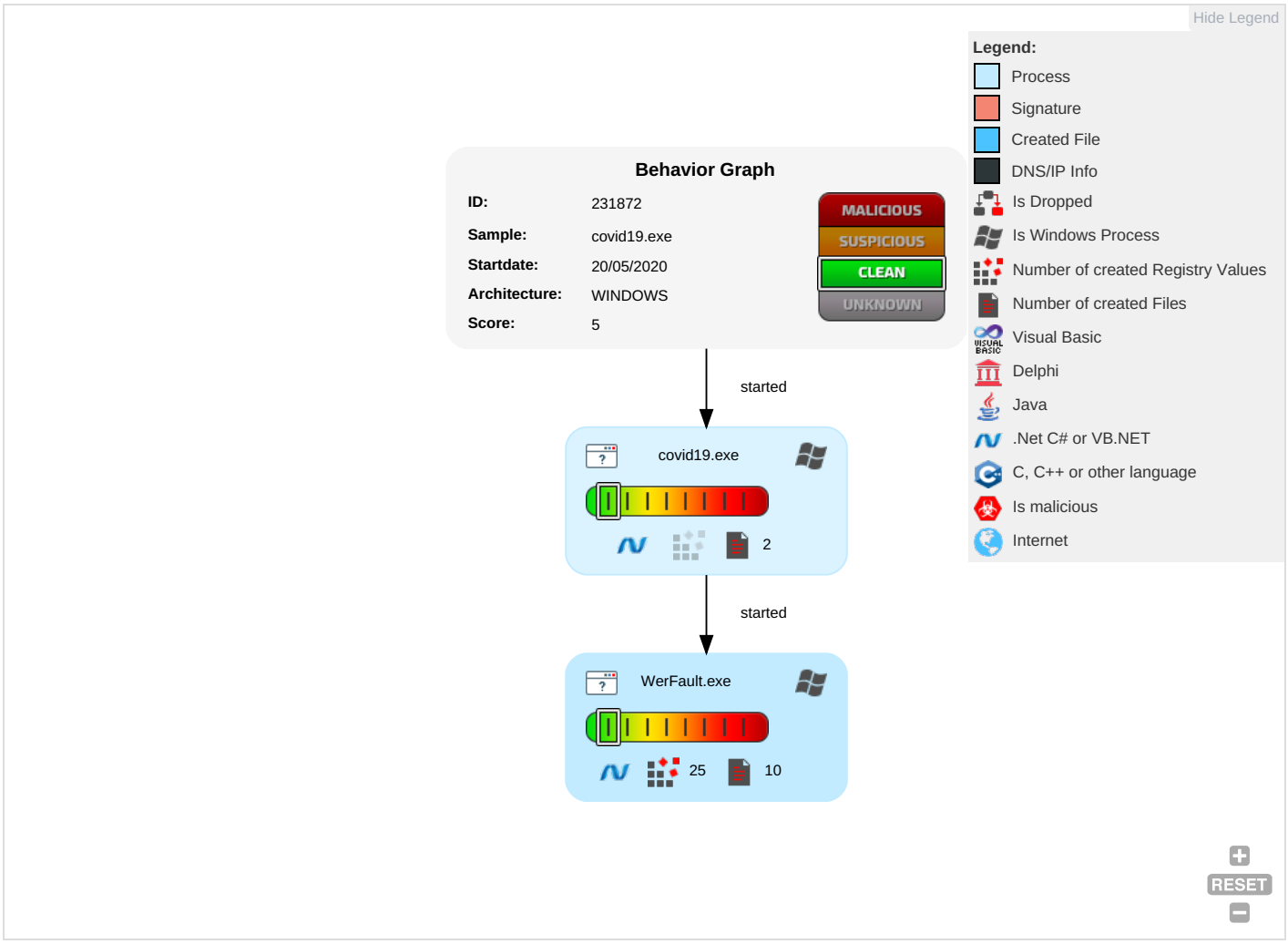


Click to jump to signature section

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 Communi
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Software Packing 2	Network Sniffing	Process Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS Redirect F Calls/SMS
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Disabling Security Tools 1	Input Capture	Security Software Discovery 2	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS Track Dev Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Virtualization/Sandbox Evasion 2	Credentials in Files	System Information Discovery 2 2	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	Manipulat Device Communi
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 Denial of Service
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Obfuscated Files or Information 2	Two-Factor Authentication Interception	Network Sniffing	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Rogue Wi Access P

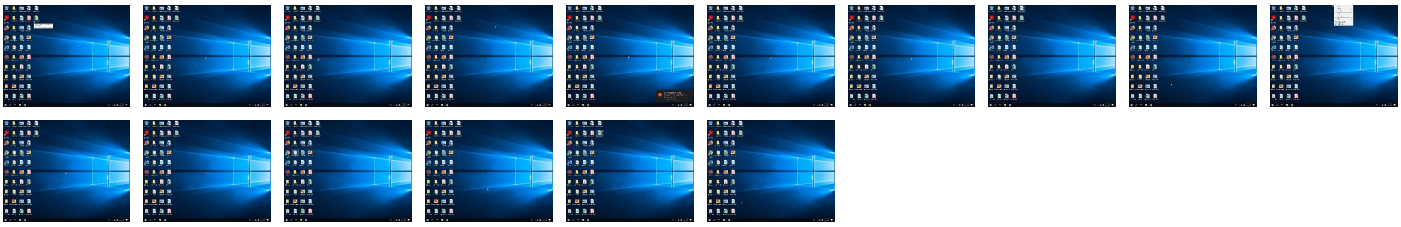
Behavior Graph



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
covid19.exe	4%	Virustotal		Browse
covid19.exe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dimonvideo.ru/uploader/488459	covid19.exe	false		high
http://https://worldometers.info/coronavirus	covid19.exe	false		high
http://https://dimonvideo.ru/0/name/c1cl0n	covid19.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	covid19.exe, 00000000.00000002.786586090.0000000002E00000.00000004.00000001.sdmp	false		high
http://https://newtonsoft.com/json	covid19.exe	false		high
http://https://dimonvideo.ru/uploader/488459)Microsoft	covid19.exe	false		high
http://https://html-agility-pack.net	covid19.exe	false		high
http://https://worldometers.info/coronavirusa//	covid19.exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	28.0.0 Lapis Lazuli
Analysis ID:	231872
Start date:	20.05.2020
Start time:	19:10:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	covid19.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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean5.winEXE@2/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20% (good quality ratio 14.7%) • Quality average: 38.3% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, WMIADAP.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 20.44.86.43, 104.103.81.66, 8.253.207.121, 8.241.121.254, 8.241.122.126, 67.26.83.254, 67.27.158.254 • Excluded domains from analysis (whitelisted): umwatson.trafficmanager.net, fs.microsoft.com, audownload.windowsupdate.nsatc.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net • Execution Graph export aborted for target covid19.exe, PID 1096 because it is empty • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:11:24	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\Report.wer

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

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Size (bytes):	13604
Entropy (8bit):	3.7966002186357977
Encrypted:	false
MD5:	C8EA1DD4EBB65F66C56BAB785EC15F4C
SHA1:	FD402E195AC3E76AB22AD0AE566817E942839CC6
SHA-256:	FB4DD7D371A71C4284ECC55B032083F0775268B6E163653B091BEE660EB00878
SHA-512:	F2E0494EBB5D09D58C73580DFF02C08526D6B8D0EB27F081DBB7B5B6F8E2591841C1FC8156379C4ED57F7BC4101C1E1BC85DEB86DDDBC785B9F33AC6E1550 D
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.3.4.5.0.0.6.8.2.6.2.3.7.4.8.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.3.4.5.0.0.6.8.4.0.1.0.6.0.8.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.8.6.5.0.4.a.a.-.0.7.6.6.-.4.8.d.9.-.8.6.9.a.-.c.6.f.0.d.0.d.d.a.9.a.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.b.1.e.1.6.a.c.-.5.d.2.c.-.4.3.4.9.-.a.e.7.0.-.9.6.5.0.f.1.0.7.8.0.1.c.....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.=.c.o.v.i.d.1.9...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.c.o.v.i.d.1.9...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.4.4.8.-.0.0.0.1.-.0.0.1.b.-.4.7.1.8.-.9.9.1.d.1.5.2.f.d.6.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.e.5.5.5.e.6.6.0.1.5.5.5.b.d.0.7.3.a.f.e.1.1.c.f.e.2.d.4.d.1.b.0.0.0.0.0.0.0.0.0.!.0.0.0.0.4.0.1.2.7.9.d.a.5.7.7.7.3.a.1.4.8.f.d.e.2.8.8.6.3.0.8.f.5.6.8.c.9.9.0.1.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu May 21 02:11:23 2020, 0x1205a4 type
Size (bytes):	226139
Entropy (8bit):	4.2276481926377745
Encrypted:	false
MD5:	6F79140B5E9EC3B5D0C0BEA0811BE106
SHA1:	57A6E85491BE3676932DCB59A99FA2DB2FD067E3
SHA-256:	BA5B79EB796A1B495E5A649663A7B625196BAD6A5E948B9D338D25D65BE11180
SHA-512:	2B3A6ED479F90FE0A63D737B80BBDE03661F83DBDF5DA5DA4AC9506C97DAE381E666362EA08524659591401A2EB50051FFA630932882D95ABFD72236987D2392
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....K..^.....?.....B.....`.....GenuineIntel.....T.....H...G..^.....0.....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\WER65E9.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):	8350
Entropy (8bit):	3.689381260296304
Encrypted:	false
MD5:	1A3BCAC2B1CF38DB85B85D3394802B16
SHA1:	84973CAA6FD145341A337E726049127C90CA30D6
SHA-256:	B12C75B779EDAFFA45493622ADC0C4D5D6D4B5879F3CE18382D1111D5C460ED5
SHA-512:	48D0927512AC4A83729CDF701049BBF657AC57A948D2E7DD1C2713CB62D98D0A7D977399D078FCC5777FD4A06BDD405008C8631AB53FAE09458A131AFAAF9A5
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.>.1.0.9.6.<./.P.i.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Size (bytes):	4672
Entropy (8bit):	4.431259990581435
Encrypted:	false
MD5:	3E1641CCBEC61700BC0A79BE9D74E53E
SHA1:	6EAD1ACAF87097056F7A74F3FE9F090507D771C0
SHA-256:	CA4BF42C8BC7F00B920835BE095FAB871601D2CB41EABB7A14B7CB61BE810167

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp.xml	
SHA-512:	263DE2E337F6BA05E5C3355CFA23CAF0540D9F26E9B457A958C723762CEAC26CC68102ADDD638BB653A354FF76E960C1CE82D8458FE5ADC83A2365CBA874EF E
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="977348" />.. <arg nm="osinsty" val="2" />.. <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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.40262402459457
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	covid19.exe
File size:	1151488
MD5:	d0a7273fc33b37a38336213b86def543
SHA1:	401279da57773a148fde2886308f568c9901054a
SHA256:	27725450780b19dd823f2ad601a6038442d3da4d9bbade3f16ee5e037b28f452
SHA512:	42eadb7239278b7496d4a1031fb819306d60c27c41f303e4f9b051a86b9ae194a1e478abb7e803430c6241dd6712ab2cd5edc05dfd629d537651a47d35fd9d4f
SSDEEP:	12288:632BjQL4hM0JJLwM8aT1QL4hM0JJLwM8aT1QL4hM0JJLwM8aT9mJlBko9AQgohQd:VHrGOprGOprGOElOomFo5r4O
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....P.....|.....3... ...@....@.. .....`.....

File Icon

Icon Hash:	f0ccc66785e4c070

Static PE Info

General

Entrypoint:	0x4e3312
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5EBCA39A [Thu May 14 01:49:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General	
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe32c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x37968	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x11c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe3188	0x1c	.text
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe1318	0xe1400	False	0.815455700264	data	7.43476856318	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x37968	0x37a00	False	0.808457689607	data	7.27550218121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe41a0	0x1ec46	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x102df8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x113630	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x117868	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x119e20	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x11aed8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x11b350	0x5a	data		
RT_VERSION	0x11b3bc	0x3ac	data		
RT_MANIFEST	0x11b778	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright c1cl0n, 2020
Assembly Version	5.2.0.0
InternalName	covid19.exe
FileVersion	5.2.0.0
CompanyName	
LegalTrademarks	
Comments	.
ProductName	covid19
ProductVersion	5.2.0.0
FileDescription	covid19 - .
OriginalFilename	covid19.exe

Network Behavior

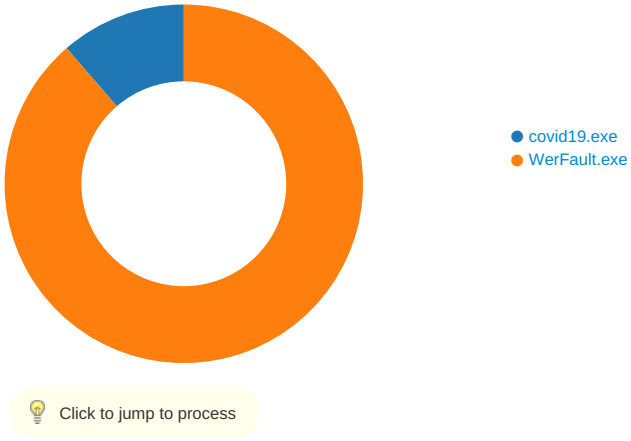
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 20, 2020 19:11:24.606513977 CEST	55729	53	192.168.2.5	8.8.8.8
May 20, 2020 19:11:24.632015944 CEST	53	55729	8.8.8.8	192.168.2.5
May 20, 2020 19:11:38.221067905 CEST	56104	53	192.168.2.5	8.8.8.8
May 20, 2020 19:11:38.342217922 CEST	53	56104	8.8.8.8	192.168.2.5
May 20, 2020 19:12:03.016995907 CEST	62623	53	192.168.2.5	8.8.8.8
May 20, 2020 19:12:03.042265892 CEST	53	62623	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: covid19.exe PID: 1096 Parent PID: 4320

General

Start time:	19:11:19
Start date:	20/05/2020
Path:	C:\Users\user\Desktop\covid19.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\covid19.exe'
Imagebase:	0x9f0000
File size:	1151488 bytes
MD5 hash:	D0A7273FC33B37A38336213B86DEF543
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D4EA9F6	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D4EA9F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D493625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\5e7364da399b604ae01baff696551080\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3FEE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D49A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D49A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D49A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D49A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D49A974	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\84b9171c43be8428a7ceaf253e5d7738\System.ni.dll.aux	unknown	620	success or wait	1	6D3FEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\d88a90d2c98cca1a9d491dfeb73352be\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3FEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\2da4cf2bb9a8f8a554da96d83ee20d39\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3FEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4d91b386e64bacbfdf3b2db16155386b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3FEE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D493625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Users\user\Desktop\covid19.exe	unknown	4096	success or wait	1	6D4D28CF	unknown
C:\Users\user\Desktop\covid19.exe	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Users\user\Desktop\covid19.exe	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Users\user\Desktop\covid19.exe	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Users\user\Desktop\covid19.exe	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D4D28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D4D28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D4D28CF	unknown

Analysis Process: WerFault.exe PID: 1624 Parent PID: 1096

General

Start time:	19:11:21
Start date:	20/05/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1096 -s 1040
Imagebase:	0x11f0000
File size:	434584 bytes
MD5 hash:	80E91E3C0F5563E4049B62FCAF5D67AC

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
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	732E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	732D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	success or wait	1	732D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	success or wait	1	732D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp.xml	success or wait	1	732D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6665.tmp.csv	success or wait	1	732D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER678F.tmp.txt	success or wait	1	732D4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 4b e3 c5 5e a4 05 12 00 00 00 00 00	MDMP..... .....K..^.....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.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 60 1f 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 48 04 00 00 47 e3 c5 5e 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 0d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....?...........B......`..... ..GenuineIntel............T... ....H...G..^.................. ....0.................. 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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.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 01 00 00 00 00 ef ef 00 05 00 00 00 00 00 00 00 05 00 00 00 40 ee ef 00 98 ee ef 00 c2 dd 5d 77 23 00 00 00 12 02 00 00 40 ee ef 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+......................@... ......]w#.......@...+.........	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	168	d0 10 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 c2 dd 5d 77 00 00 00 00 05 00 00 00 00 00 00 00 09 15 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3b 6d 00 00 00 00 a0 0c 1d 01 00 00 00 00 54 ef ef 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 69 fe 00 00 00 00 00 10 8a 3c 6d 00 00 00 00 0b 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 29 01 14 01 00 00 00 00 60 ee ef 00 00 00 00 00 cc 02 00 00 62 25 00 00	........RCC...............]w.. ....;m............T. ....i........ <m....................)..... ..`...........b%..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	20	05 02 00 00 60 36 1f 01 00 00 00 00 04 00 00 00 7e 56 00 00	....`6..........~V..	success or wait	517	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	4	78 18 0c 77	x..w	success or wait	516	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	176	00 00 1f 01 c8 16 1d 01 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 00 00 00 c0 18 d2 a3 6d 70 2f 1f 01 00 00 00 00 00 10 02 6c 38 2c 1f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 06 00 00 00 80 d8 a3 6d 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 38 1a 1d 01 e8 b9 1e 01 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	....mp/.........l8,...... ....m............ ....8.....................	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 98 e6 ef 00 bc a7 8e 77 23 00 00 00 02 02 00 00 08 e5 ef 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#...........+.........	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	48	08 11 00 00 01 00 00 00 20 00 00 00 02 00 00 00 00 90 c7 00 00 00 00 00 08 fa f9 04 00 00 00 00 f8 05 00 00 3d 64 01 00 cc 02 00 00 5e 33 00 00	....=d......^3..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	4	31 00 00 00	1...	success or wait	49	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	28	16 00 00 00 63 00 6f 00 76 00 69 00 64 00 31 00 39 00 2e 00 65 00 78 00 65 00 00 00	....c.o.v.i.d.1.9...e.x.e...	success or wait	49	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	120	00 00 50 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 24 25 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 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 0c 00 00 00 18 00 00 00 01 00 00 00	..Pj............`.Z$%........ ....?........... ....).............. ..@A.........................	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	24	12 00 00 00 70 00 73 00 61 00 70 00 69 00 2e 00 64 00 6c 00 6c 00 00 00	....p.s.a.p.i...d.l.l...	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	668	00 00 34 74 00 00 00 00 00 60 00 00 f9 0a 01 00 51 32 d9 44 4a 25 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 04 00 00 00 00 80 39 02 00 00 00 00 00 60 c8 02 00 00 00 00 cf 12 05 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 4e b6 03 00 00 00 00 00 0a 1b 05 00 00 00 00 00 4d 0d 02 00 00 00 00 00 c6 d4 1b 00 00 00 00 00 7a 2a 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 fb a0 04 00 00 00 00 00 e0 36 cc bc 00 00 00 00 d2 7d a3 66 00 00 00 00 00 46 d2 92 0e 00 00 00 00 8f 3f f4 00 00 00 00 00 ee e2 03 00 fa c0 00 00 23 4e 05 00 58 91 03 00 7a 2a 04 00 8d ff 10 00 fb a0 04 00 16 40 2c 00 9d 5f 01 00 8f 28 14 00 00 00 00 00 01 95 13 00 a4 f9 06	..4t.....`......Q2.DJ%......Zb ..... .....9.....` .....N... .....M.....z* .....@.....6..... .}.f....F.....?..... ..#N..X...z*.....@,..._... (.....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	16492	0c 00 00 00 4d 00 75 00 74 00 61 00 6e 00 74 00 00 00 00 00 00 00 02 00 00 00 08 00 00 00 01 00 00 00 00 00 00 49 33 03 00 03 00 00 00 08 00 00 00 00 00 00 00 00 00 00 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 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	....M.u.t.a.n.t..... ....I3..... ..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	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER627D.tmp.dmp	unknown	120	03 00 00 00 f4 00 00 00 08 07 00 00 04 00 00 00 b0 14 00 00 08 08 00 00 0e 00 00 00 24 00 00 00 b8 1c 00 00 05 00 00 00 54 20 00 00 2a 36 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 00 29 00 00 a3 4a 03 00 15 00 00 00 ec 01 00 00 dc 1c 00 00 16 00 00 00 98 00 00 00 c8 1e 00 00	.....$.....T ..*6.....`... ....8.....T.....) ...J.....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 30 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.0.9.6.<./.P.i.d.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6f 00 76 00 69 00 64 00 31 00 39 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.c.o.v.i.d.1.9...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.3.7.0.<./.U.p.t.i.m.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 35 00 36 00 31 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.9.5.6.1.6.7.6.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 33 00 36 00 32 00 36 00 31 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.9.3.6.2.6.1.1.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 37 00 30 00 36 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.>.7.0.6.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 32 00 33 00 34 00 32 00 35 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.3.4.2.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 32 00 33 00 34 00 32 00 35 00 30 00 32 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.>.2.3.4.2.5.0.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 33 00 30 00 35 00 38 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.>.3.0.5.8.2.4.<./.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 33 00 30 00 35 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.5.8.2.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.4.2.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.1.0.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 31 00 32 00 32 00 31 00 30 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.2.2.1.0.1.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 31 00 32 00 32 00 31 00 38 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.2.2.1.8.3.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 31 00 32 00 32 00 31 00 30 00 31 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.2.2.1.0.1.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.9.2.8.<./.P.i.d.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 32 00 31 00 32 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.6.2.1.2.2.3.<./.U.p.t.i.m.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 36 00 30 00 38 00 35 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.6.0.8.5.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 39 00 38 00 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.8.8.8.5.6.3.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 39 00 38 00 35 00 32 00 35 00 31 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.>.9.8.5.2.5.1.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 30 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.0.9.7.6.<./.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 36 00 36 00 38 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.>.9.3.6.6.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 38 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.7.8.3.5.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 37 00 34 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.>.7.7.4.8.8.<./.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 34 00 39 00 38 00 38 00 30 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.9.8.8.0.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 36 00 35 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.7.6.5.6.9.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 34 00 39 00 38 00 38 00 30 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.9.8.8.0.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 63 00 6f 00 76 00 69 00 64 00 31 00 39 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.>.c.o.v.i.d.1.9...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 6a 00 6f 00 76 00 62 00 6c 00 6a 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.>.y.j.o.v.b.l.j. .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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 68 00 71 00 6c 00 6d 00 6e 00 74 00 63 00 6c 00 65 00 6b 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.h.q.l.m.n.t.c.l.e.k.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 68 00 71 00 6c 00 6d 00 6e 00 74 00 63 00 6c 00 65 00 6b 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.>.h.q.l.m.n.t.c.l.e.k.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 34 00 39 00 35 00 38 00 33 00 33 00 34 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.4.9.5.8.3.3.4.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 35 00 2d 00 32 00 31 00 54 00 30 00 32 00 3a 00 31 00 31 00 3a 00 32 00 33 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.0.5.-.2.1.T.0.2.:.1.1.:.2.3.Z.".>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	262	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 34 00 30 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 30 00 39 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 32 00 32 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 31 00 35 00 32 00 32 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 4.0.5.". .P.I.D.=.".1.0.9.6.". .U.p.t.i.m.e.M.S.=.".1.5.2.2.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.5.2.2.". .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.=."	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 38 00 36 00 35 00 30 00 34 00 61 00 61 00 2d 00 30 00 37 00 36 00 36 00 2d 00 34 00 38 00 64 00 39 00 2d 00 38 00 36 00 39 00 61 00 2d 00 63 00 36 00 66 00 30 00 64 00 30 00 64 00 64 00 61 00 39 00 61 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.8.6.5.0.4.a.a.-.0.7.6.6.-.4.8.d.9.-.8.6.9.a.-.c.6.f.0.d.0.d.d.a.9.a.b.<./.G.u.i.d.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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 35 00 2d 00 32 00 31 00 54 00 30 00 32 00 3a 00 31 00 31 00 3a 00 32 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.0.5.-.2.1.T.0.2.:.1.1.:.2.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER65E9.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	732D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6657.tmp.xml	unknown	4672	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	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\Report.wer	unknown	2	ff fe	..	success or wait	1	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\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	182	732D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_covid19.exe_b03463187c65eb64202a8a1ae95098aa13a7e25c_b968a014_06026ba4\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 34 00 31 00 34 00 34 00 36 00 35 00 32 00 35 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.4.1.4.4.6.5.2.5.1.	success or wait	1	732D497A	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	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	success or wait	1	732F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	732F1FB2	RegCreateKeyExW
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	732D43D1	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	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{8ce9bf7a-72be-4262-a9a7-d698cb90f972}	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	ProgramId	unicode	0006e555e6601555bd073afe11cfe2d4d1b000000000	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	FileId	unicode	0000401279da57773a148fde2886308f568c9901054a	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	LowerCaseLongPath	unicode	c:\users\user\desktop\covid19.exe	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	LongPathHash	unicode	covid19.exe|1fdce17a	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Name	unicode	covid19.exe	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Publisher	unicode		success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Version	unicode	5.2.0.0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	BinFileVersion	unicode	5.2.0.0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	BinaryType	unicode	pe32_clr_32	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	ProductName	unicode	covid19	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	ProductVersion	unicode	5.2.0.0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	LinkDate	unicode	05/14/2020 01:49:14	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	BinProductVersion	unicode	5.2.0.0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Size	B	00 92 11 00 00 00 00 00	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Language	dword	0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	IsPeFile	dword	1	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	IsOsComponent	dword	0	success or wait	1	732F36BF	unknown
\REGISTRY\A\{970dc78d-2202-d7aa-cf28-7632caa06905}\Root\InventoryApplicationFile\covid19.exe|1fdce17a	Usn	B	B8 FC 2B 0A 00 00 00 00	success or wait	1	732F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 C2 DD 5D 77 05 00 00 00 09 15 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3B 6D A0 0C 1D 01 54 EF EF 00 01 00 00 00 00 00 00 00 00 B4 69 FE 00 10 8A 3C 6D 0B 00 00 00 01 00 00 00 29 01 14 01 60 EE EF 00	success or wait	1	732F1FE8	RegSetValueExW

Disassembly

Code Analysis