ID: 392881
Sample Name: qMus8K6kXx.dll
Cookbook: default.jbs
Time: 23:43:30
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report qMus8K6kXx.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
E-Banking Fraud: 5
Malware Analysis System Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 11
Static PE Info 11
General 12
Entrypoint Preview 12
Data Directories 12
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 14
Code Manipulations 14
Statistics 14

Behavior 14
System Behavior 14
Analysis Process: loaddll32.exe PID: 1536 Parent PID: 5652 14
General 14
File Activities 15
Analysis Process: cmd.exe PID: 1240 Parent PID: 1536 15
General 15
File Activities 15
Analysis Process: rundll32.exe PID: 6072 Parent PID: 1240 15
General 15
File Activities 15
File Read 15
Analysis Process: rundll32.exe PID: 4720 Parent PID: 1536 15
General 15
File Activities 16
File Read 16
Analysis Process: WerFault.exe PID: 5792 Parent PID: 1536 16
General 16
File Activities 16
File Created 16
File Deleted 17
File Written 17
Registry Activities 39
Key Created 39
Key Value Created 39
Disassembly 39
Code Analysis 40

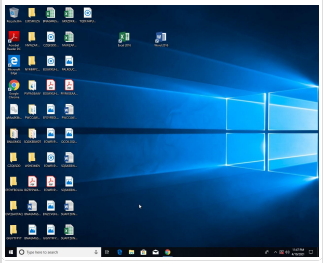
Analysis Report qMus8K6kXx.dll

Overview

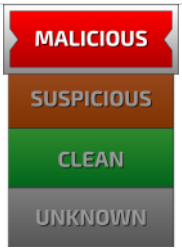
General Information

Sample Name:	qMus8K6kXx.dll
Analysis ID:	392881
MD5:	a789cbe1be2a6e..
SHA1:	d70b6c72da60fa4.
SHA256:	01c6da823713ae..
Tags:	40111 Dridex
Infos:	

Most interesting Screenshot:



Detection



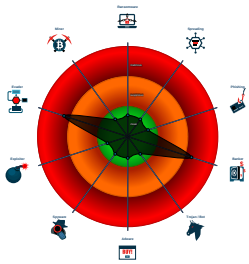
Dridex Dropper

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

Signatures

- Dridex dropper found
- Machine Learning detection for samp…
- Tries to delay execution (extensive O…
- Tries to detect sandboxes / dynamic…
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec…
- Creates a process in suspended mo…
- Found a high number of Window / Us…
- One or more processes crash
- Sample execution stops while proce…
- Sample file is different than original …
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 1536 cmdline: loaddll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 1240 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6072 cmdline: rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4720 cmdline: rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',ReadLogRecord MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 5792 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1536 -s 416 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

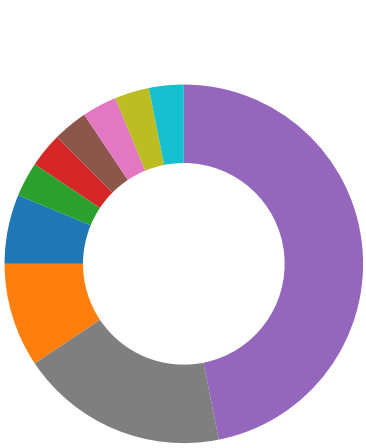
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

E-Banking Fraud:

Dridex dropper found

Malware Analysis System Evasion:

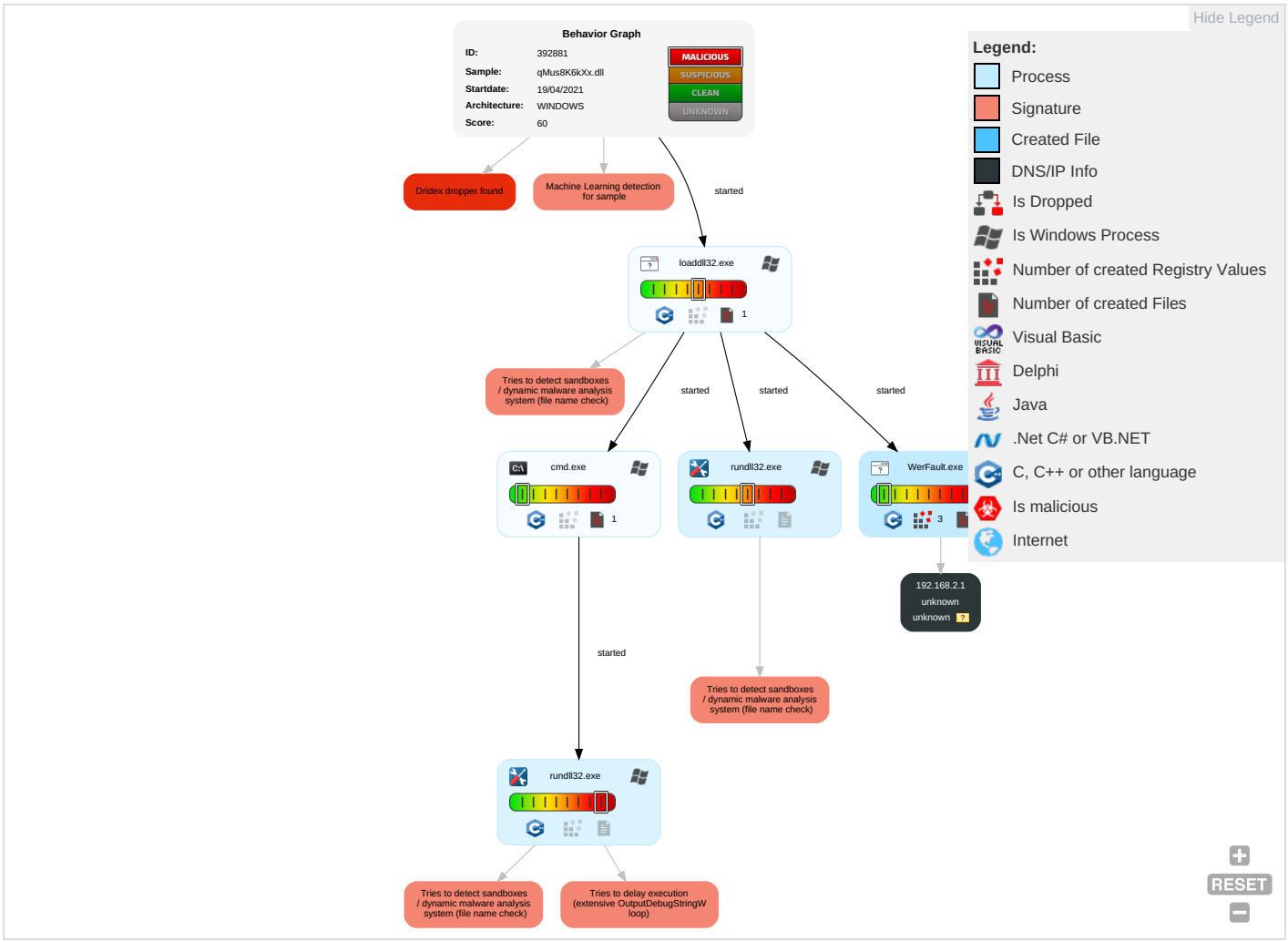
Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes / dynamic malware analysis system (file name check)

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 Management Instrumentation	Path Interception	Process Injection 1 1	Rundll32 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 3	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

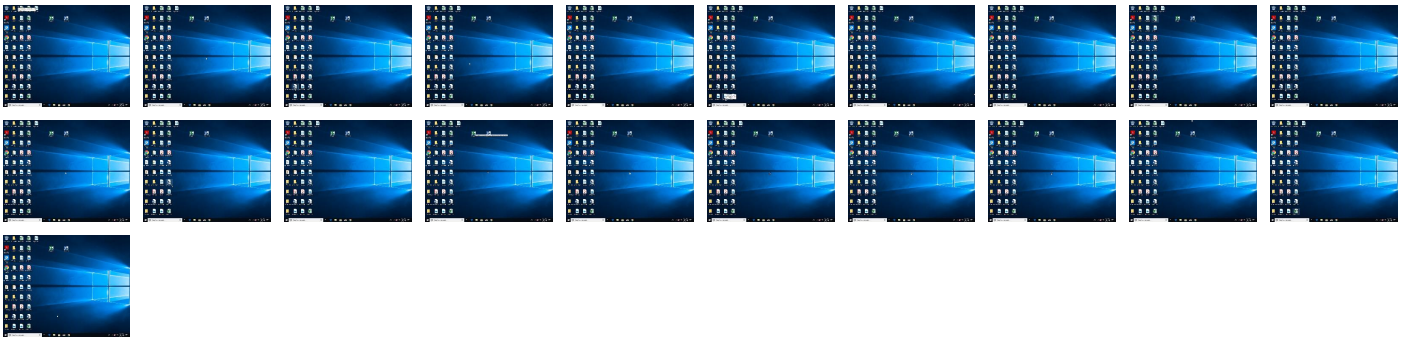
Behavior Graph



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
qMus8K6kXx.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.ec0000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

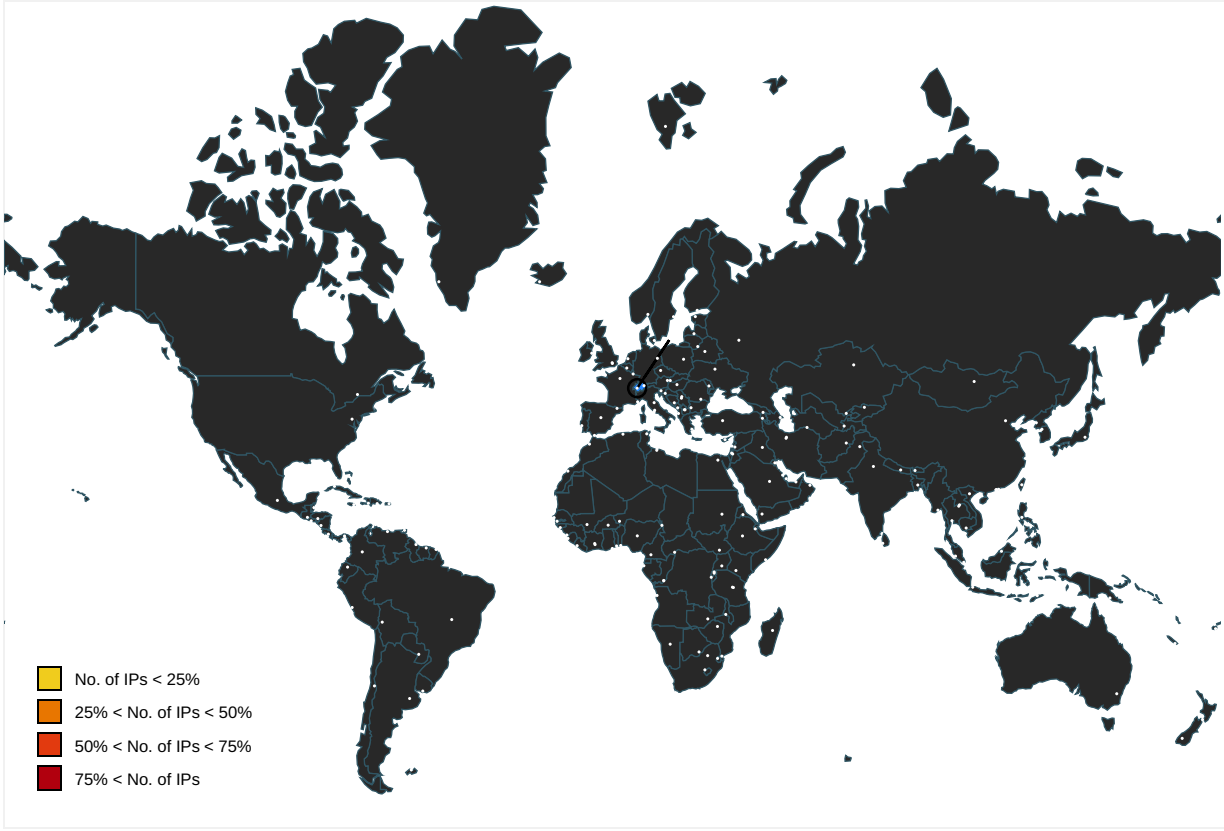
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ansicon.adoxa.vze.com/6	qMus8K6kXx.dll	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392881
Start date:	19.04.2021
Start time:	23:43:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	qMus8K6kXx.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.bank.evad.winDLL@8/4@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.6% (good quality ratio 61.9%) • Quality average: 61.5% • Quality standard deviation: 47.6%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, WerFault.exe, wermgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/392881/sample/qMus8K6kXx.dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	9232
Entropy (8bit):	3.7640828500326498
Encrypted:	false
SSDEEP:	96:kozXyjy9hAvC5Q56tpXIQcQ6c6n+hcEZcw3P+a+z+HbHgi6eugtYsaV9w7kkoUPB:AwHUb+hjbjZq/u7sPS274Itb2P
MD5:	966824EFBF856BB59479BC30B6AF2ED3
SHA1:	28C2BA9D059D8D329EF3F6D37FC234089E36F9B8
SHA-256:	4B32DB4C094AF59556D65A7785273DF98C638F9A306B7DB5F33771BCC2066A4E
SHA-512:	EFFFB8C2D4B6318438A1E2F5E5E4AE45BBE3F8456A6B2B2C8E611B0C88C15E0F4EB96C90689E38B8D9A4500A6DA448CDE9CDAB80E16E547F8098023055FDD6B7
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.3.3.7.4.8.2.2.3.3.1.6.4.9.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.0.9.c.0.c.8.7.-.c.c.c.0.-.4.c.e.7.-.8.c.8.f.-.6.1.4.2.3.8.7.8.6.6.f.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.c.9.d.3.c.a.9.-.4.a.8.b.-.4.8.2.b.-.a.8.4.3.-.c.1.9.5.9.e.7.6.8.1.2.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.0.0.-.0.0.0.1.-.0.0.1.7.-.7.2.c.4.-.f.e.9.6.b.0.3.5.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.4././.0.4.:.1.0.:.5.0.:.5.4.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Apr 20 06:47:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	24938
Entropy (8bit):	2.654289963144762
Encrypted:	false
SSDEEP:	192:eQ7qmBgqtDUft2hPiyNUvxps24Pf+kTkgv9NpDi4m:Mn/AEQZTkgv9Ptm
MD5:	F80F9A52DED7BAAE6BFAEFBCFF536896
SHA1:	104C03D205AEE6A139474758470393D6B8D36451
SHA-256:	A9EBDB5A762C4695A9541E9AAF50F86BB5CC2DC69F8B97FE187D360AE7033262
SHA-512:	129C5DADC1722F52CBF2635F6B371AE0D76BED5165DFE89747379AEFFB8DBE9EEC4398B60B2A38D4D06C36A76656B2BB62F23D83925E5C0077233DEC2F35E3F
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....x~`.....U.....B.....,.....GenuineIntelW.....T.....Cx~`.....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\WER530B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8358
Entropy (8bit):	3.6955773728043133
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNir66UKa6YSwSUM4gmfwS1dCpB489bknrsfPsm:RrlsNim6UKa6YlSUM4gmfwS1Sknwfx
MD5:	8D7126D39B56CA77FA5940BCCB47815E
SHA1:	BFCE41016E6FDBD70C13525460E84DA6AB59AE61
SHA-256:	7AF4E915E3CA39BDE972CA28DB62E10DD66DBE820B80B98540F608006087D471
SHA-512:	88CFE9C8892A661803A0354B9F604C7D17B498962219EF1DC6879644EA773E4D146A7570705455C40ADD4DB008C76B2BB43A20D3CC496B3D3DE7D5314847DFC
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.5.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4658
Entropy (8bit):	4.427583601313243
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI90AY6WSC8BtB8fm8M4JVFFPHw+q8v71uKcQIcQw6Urgd:uITfqLAY7SN3GJ9QKZuKkw68gd
MD5:	4483C95BA3FBD0C4BB13B9CD5207EE06
SHA1:	38D8DE818281A494A320F029C3C17CD0B2AEEE5D
SHA-256:	F7EC05C774D1B8D58A5E25DDB355B91FA54CD18B12DE7C4F4817A14A12346BA9
SHA-512:	073D7C735220E94517BAB0F227A8351F6BE8A57B10C0144D1F5DB129E09252CF3491BFA294769830040E52FBCD05E97F9414F569F0FF9923638FF7CCBBA4CAF7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="954237" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.5485540145940595
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	qMus8K6kXx.dll
File size:	163840
MD5:	a789cbe1be2a6e99de90f65c5213c992
SHA1:	d70b6c72da60fa4dc4c2b0ec32bcc41887721535
SHA256:	01c6da823713aeb976fea61d010524859d104cba25fe2570855f21828df32086
SHA512:	e1c41d50a5cf9070ab11620b15b09cfd1f6162d29352b03086731d922938bc88a68f75a824ad110d3f2068f76def0c86dab25d77f050b054a4028bd5c279f49e
SSDEEP:	3072:rWX2IjzzpM+PncPeY8+O3AU3HRIHPh3UGfXy0BHNkIv/ScbQQ2y0iNM0+y+N0tc:r42IfzNPnoeY8j3AsHGPXpHNj6rByM3
File Content Preview:	MZ.....@.....{}..{}..{}..{}...}..@.2..|..=.T..}....S.z|..@..._}..|...T|..V/C..|..V/E..|..Rich[}.....PE..L.....}`.....!.....f.....D.....P....@..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x424410
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x607DE4E3 [Mon Apr 19 20:15:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b84fd50f2389cfd5bd83e2cf062986d1

Entrypoint Preview

Instruction
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp edx, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
je 00007F17F0A15AABh
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1001	0x0	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2768c	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x340	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x14c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x25040	0x38	.rdata
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	0x25000	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2356e	0x23600	False	0.761560015459	data	7.55877156847	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2842	0x2a00	False	0.791573660714	data	7.53164670284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x28000	0x3588	0x1600	False	0.783380681818	MMDF mailbox	7.34765964879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x340	0x400	False	0.390625	data	2.73456990044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x14c	0x200	False	0.62890625	data	4.21021599876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x2e0	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, OpenSemaphoreW, LoadLibraryExA, GetModuleHandleW, OutputDebugStringA, GetProfileSectionW
OPENGL32.dll	glTexSubImage1D
ole32.dll	CreateStreamOnHGlobal
USER32.dll	TranslateMessage
ADVAPI32.dll	RegLoadAppKeyW

Version Infos

Description	Data
LegalCopyright	Freeware
InternalName	ANSI32
FileVersion	1.66
CompanyName	Jason Hood
Comments	http://ansicon.adoxa.vze.com/
ProductName	ANSICON
ProductVersion	1.66
FileDescription	ANSI Console
OriginalFilename	ANSI32.dll
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

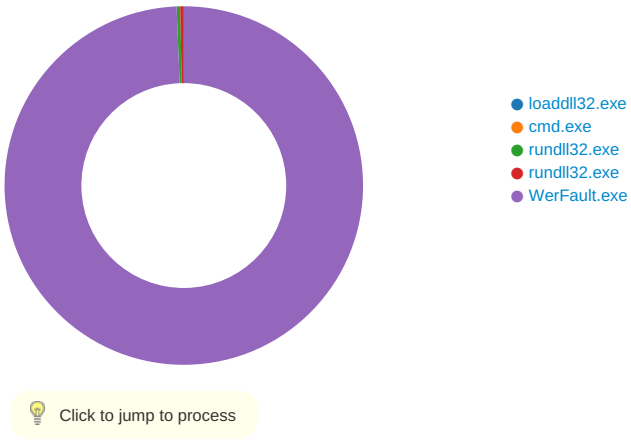
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 1536 Parent PID: 5652

General

Start time:	23:44:19
Start date:	19/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll'
Imagebase:	0x150000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1240 Parent PID: 1536

General

Start time:	23:44:19
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6072 Parent PID: 1240

General

Start time:	23:44:20
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',#1
Imagebase:	0x1200000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6FAF5E36	ReadFile

Analysis Process: rundll32.exe PID: 4720 Parent PID: 1536

General

Start time:	23:44:56
Start date:	19/04/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\qMus8K6kXx.dll',ReadLogRecord
Imagebase:	0x1200000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6FAF5E36	ReadFile

Analysis Process: WerFault.exe PID: 5792 Parent PID: 1536

General

Start time:	23:46:58
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1536 -s 416
Imagebase:	0x1000000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	702D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp.xml	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER584A.tmp.csv	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7028.tmp.txt	success or wait	1	702C497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 e7 78 7e 60 a4 05 12 00 00 00 00 00	MDMP..... .....x~`.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 2c 14 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 00 06 00 00 43 78 7e 60 09 00 00 00 16 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00	.....U.....B.....,..... ..GenuineIntelW.....T... .....Cx~`..... .....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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 ae 6f b0 f9 8f 00 00 00 00 00 00 00 ae 6f 00 00 ae 6f 00 00 00 00 bc f9 8f 00 00 00 ae 6f 23 00 00 00 46 02 01 00 a0 f9 8f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+......o..........o...o.... ....o#...F.......+.........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	168	0c 0d 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ae 6f 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 ae 6f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 30 17 00 00	..........................o.. ....o........ ....0...	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	20	06 00 00 00 c4 eb 8f 00 00 00 00 00 3c 14 00 00 2c 1d 00 00	...........<...,...	success or wait	6	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	5180	bc 9a e5 77 f2 1d ea 77 aa aa aa aa f8 eb 8f 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 4c f1 8f 00 00 00 00 00 9c 01 00 00 00 00 00 00 00 00 00 00 00 9c 01 00 00 c4 01 00 00 90 ec 8f 00 aa aa aa aa 90 ec 8f 00 12 12 ea 77 c4 01 00 00 00 00 00 00 aa aa aa aa f4 ec 8f 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 80 ee 8f 00 30 ee 8f 00 c4 01 00 00 00 00 b0 00 04 00 00 00 a0 01 00 00 a4 01 00 00 a8 01 00 00 9c 01 00 00 00 00 00 00 9c 01 00 00 a0 01 00 00 a8 01 00 00 a4 01 00 00 aa aa aa aa 18 ec 8f 00 aa aa aa aa 44 ed 8f 00 f0 17 e6 77 aa aa aa aa 00 00 00 00 ac ec 8f 00 91 0c ea 77 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 70 fa 8f 00 3d ac e9 77 30 ee 8f 00 80 ee 8f 00 aa aa aa aa 00 00 00	...w...w..... ..L..... .....w..... ....0..... ....D.....w..... .w.....p...=..w 0.....	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	256	c2 08 00 90 b8 54 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 55 00 00 00 ba e0 dc e6 77 ff d2 c2 2c 00 90 b8 56 00 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 57 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 58 00 00 00 ba e0 dc e6 77 ff d2 c2 0c 00 90 b8 59 00 00 00 ba e0 dc e6 77 ff d2 c2 40 00 90 b8 5a 00 18 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 5b 00 1d 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 5c 00 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 5d 00 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 5e 00 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 5f 00 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 60 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 61 00 07 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 62 00 00 00 ba e0 dc e6 77 ff d2 c2 1c 00 90 b8 63 00 00 00 ba e0 dc e6 77 ff	.....T.....w.....U.....w ....,...V.....w.....W..... .w.....X.....w.....Y.... ...w...@...Z.....w.....[.. .....w.....\.....w.....] .....w.....^.....w..... ._.....w.....`.....w.... ...a.....w.....b.....w.. .....c.....w.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 ae 6f 00 00 ae 6f 00 00 00 00 08 ec 8f 00 bc 9a e5 77 23 00 00 00 02 02 00 00 c8 eb 8f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.................o...o.... ....w#...........+........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	48	0c 0d 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 e0 79 00 00 00 00 00 c4 eb 8f 00 00 00 00 00 3c 14 00 00 2c 1d 00 00 cc 02 00 00 fc 19 00 00	....y............ <...,...........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	4	18 00 00 00	....	success or wait	24	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	24	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	120	00 00 a3 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 f4 0e d4 16 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 02 00 00 00	...t.....`..A!..-a........... ....B.......B?........... ....#............. ..@A.........................	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	34	1c 00 00 00 71 00 4d 00 75 00 73 00 38 00 4b 00 36 00 6b 00 58 00 78 00 2e 00 64 00 6c 00 6c 00 00 00	....q.M.u.s.8.K.6.k.X.x...d.l.l...	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	668	00 00 ae 6f 00 00 00 00 00 10 02 00 00 00 00 00 72 49 67 60 0e 17 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 8e 01 00 00 00 00 00 90 c4 02 00 00 00 00 1d 4f 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 2d 24 02 00 00 00 00 00 16 79 03 00 00 00 00 00 90 53 01 00 00 00 00 00 da 80 01 00 00 00 00 00 66 7e 1e 00 00 00 00 00 40 ff 1f 00 00 00 00 00 5c 94 1e 00 00 00 00 00 a2 bb d3 46 00 00 00 00 1f 48 1e 1f 00 00 00 00 07 15 a3 0d 00 00 00 00 f9 47 b4 00 00 00 00 00 86 a2 00 00 1b d5 00 00 fd 36 04 00 4d 96 02 00 66 7e 1e 00 4d fb 24 00 5c 94 1e 00 11 31 38 00 61 28 01 00 dc c9 14 00 00 00 00 00 2b 10 24 00 fa 5e 04	...o.....rIg`.....Zb ....P..... .....O.....-$.. .....y.....S.....f~ .....@.....\.....F.... .H.....G..... ...6..M...f~..M.$.\....18.a(.. .....+.$..^.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	6702	0c 00 00 00 54 00 68 00 72 00 65 00 61 00 64 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00 03 01 00 00 00 b0 67 00 70 12 00 00 d0 13 00 00 03 00 00 00 08 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 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 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	....T.h.r.e.a.d..... ......g.p..... ..F.i.l.e.....F.i.l.e..... F.i.l.e.....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	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CA2.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 24 0a 00 00 48 07 00 00 0e 00 00 00 3c 00 00 00 6c 11 00 00 05 00 00 00 64 00 00 00 c8 1c 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 c8 10 00 00 ea 50 00 00 15 00 00 00 ec 01 00 00 a8 11 00 00 16 00 00 00 98 00 00 00 94 13 00 00	....4.....$...H.....<. ..l.....d.....`... ....8.....T..... ...P.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.5.3.6.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 34 00 36 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.6.4.6.3.0.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 33 00 34 00 32 00 38 00 34 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.>.5.9.3.4.2.8.4.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 31 00 33 00 38 00 34 00 33 00 32 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.1.3.8.4.3.2.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.6.6.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 32 00 35 00 38 00 36 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.2.5.8.6.8.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 31 00 35 00 36 00 32 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.1.5.6.2.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 32 00 31 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.>.1.0.9.2.1.6.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.1.3.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.0.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.7.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 32 00 39 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.>.1.6.6.2.9.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 32 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.9.2.3.5.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 32 00 39 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.>.1.6.6.2.9.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 37 00 32 00 31 00 33 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.7.2.1.3.6.7.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 39 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.6.0.9.7.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 35 00 39 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.5.9.8.9.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 37 00 33 00 35 00 33 00 37 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.7.3.5.3.7.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 39 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.9.5.7.6.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 38 00 34 00 34 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.>.8.8.4.4.2.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.8.6.4.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 36 00 37 00 38 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.7.8.3.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 39 00 38 00 37 00 33 00 39 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.>.2.8.9.8.7.3.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 37 00 33 00 30 00 32 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.3.0.2.2.7.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 39 00 38 00 37 00 33 00 39 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.>.2.8.9.8.7.3.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 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.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 71 00 79 00 76 00 72 00 67 00 71 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.q.y.v.r.g.q.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 79 00 76 00 72 00 67 00 71 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.q.y.v.r.g.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 34 00 38 00 38 00 38 00 35 00 37 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.4.8.8.8.5.7.8.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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 42 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.B.<./.F.l.a.g.s.>.	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 32 00 30 00 54 00 30 00 36 00 3a 00 34 00 37 00 3a 00 30 00 34 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.4.-.2.0.T.0.6.:.4.7.:.0.4.Z.".>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	270	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 36 00 39 00 36 00 38 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 36 00 39 00 36 00 38 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.2.". .P.I.D.=.".1.5.3.6.". .U.p.t.i.m.e.M.S.=.".1.5.6.9. 6.8.". .T.i.m.e.S.i.n.c.e.C.r. e.a.t.i.o.n.M.S.=.".1.5.6.9.6 .8.". .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	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 30 00 39 00 63 00 30 00 63 00 38 00 37 00 2d 00 63 00 63 00 63 00 30 00 2d 00 34 00 63 00 65 00 37 00 2d 00 38 00 63 00 38 00 66 00 2d 00 36 00 31 00 34 00 32 00 33 00 38 00 37 00 38 00 36 00 36 00 66 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.4.0.9.c.0.c.8.7.-.c.c.c.0.-.4.c.e.7.-.8.c.8.f.-.6.1.4.2.3.8.7.8.6.6.f.6.<./.G.u.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 32 00 30 00 54 00 30 00 36 00 3a 00 34 00 37 00 3a 00 30 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.2.0.T.0.6.:.4.7.:.0.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER530B.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57EE.tmp.xml	unknown	4658	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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f\Report.wer	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f\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	149	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f940423413aeee195ae8a7e3bd18fce80b8b52f_160cf2be_16f7718f\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 34 00 31 00 30 00 37 00 39 00 36 00 32 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.8.4.1.0.7.9.6.2.0.	success or wait	1	702C497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{aa1511af-fda8-5142-52b9-24b624aae50c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	702E1FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 AE 6F 02 00 00 00 08 00 00 00 00 00 AE 6F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	702E1FE8	RegSetValueExW

Disassembly

Code Analysis