ID: 326331
Sample Name: Bank Swift.exe
Cookbook: default.jbs
Time: 10:03:06
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

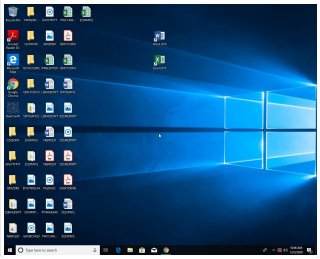
Analysis Report Bank Swift.exe

Overview

General Information

Sample Name:	Bank Swift.exe
Analysis ID:	326331
MD5:	2ace5c4532c77c…
SHA1:	c5d7fd7b905ec97..
SHA256:	53ae2502a9fed69.
Tags:	exe

Most interesting Screenshot:



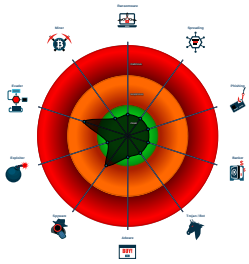
Detection

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Machine Learning detection for samp…
- PE file has a writeable .text section
- Checks if the current process is bein…
- Creates a DirectInput object (often fo…
- Enables debug privileges
- One or more processes crash
- PE file contains strange resources
- PE file does not import any functions
- Queries disk information (often used…
- Stores large binary data to the regist…
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- Bank Swift.exe (PID: 4696 cmdline: 'C:\Users\user\Desktop\Bank Swift.exe' MD5: 2ACE5C4532C77C014A02CC027D725D83)
  - WerFault.exe (PID: 5488 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4696 -s 216 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

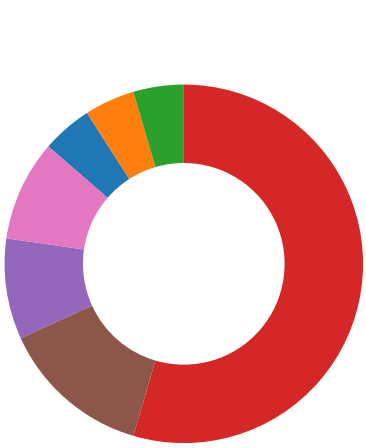
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

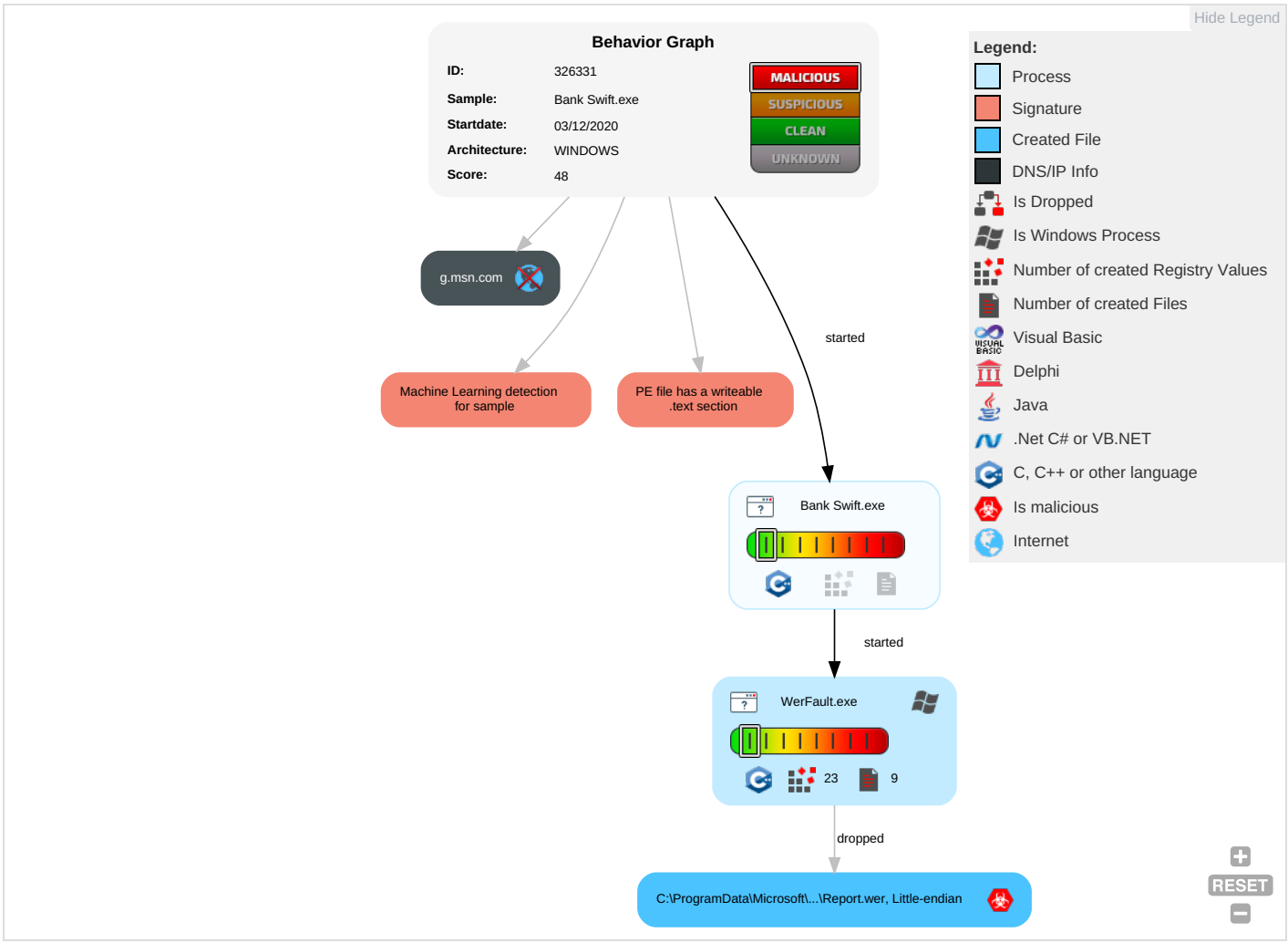
System Summary:

PE file has a writeable .text section

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Modify Registry 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

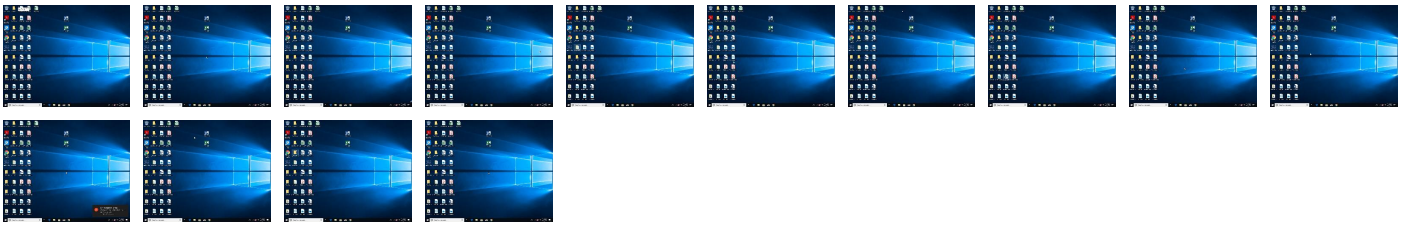
Behavior Graph



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
Bank Swift.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
g.msn.com	unknown	unknown	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326331
Start date:	03.12.2020
Start time:	10:03:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bank Swift.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
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:	mal48.winEXE@2/4@2/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.144.200, 168.61.161.212, 51.104.139.180, 13.64.90.137, 52.155.217.156, 2.20.142.210, 2.20.142.209, 51.103.5.159, 20.54.26.129, 104.43.193.48, 52.142.114.176, 92.122.213.194, 92.122.213.247, 40.88.32.150, 104.43.139.144 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Bank Swift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7398
Entropy (8bit):	3.7636306181480026
Encrypted:	false
SSDEEP:	96:ugTdVUZA4Eh8O75f0pXIQcQvc6QcEDMcw3Dpe6+HbHg6ZAXGng5FMTPSkvPkpXmd:jTvUZA4HBUZMXAjE/u7suS274It5X
MD5:	EA65043C65221DFAA6535B5E5C8D4A46
SHA1:	5B7485476F7851722DC00FF87FF426F8E2D095AC
SHA-256:	C823265D545749F44003CC1D426F0375DA2DB31B8B2EEAD56A16152FD71BBFA8
SHA-512:	812B0493EB9CE655FDE3267185DFF7FD2517A03659936DDB2AF70C7949B4CF08306A98BC91E80F6952B529FA639BCC23C0D7EA21584A4B84F66A5F612B55B885
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.1.4.9.2.2.4.4.5.9.5.5.9.0.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.1.4.9.2.2.4.7.2.5.1.8.3.7.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.b.d.0.a.4.9.b.-.b.7.1.7.-.4.8.6.0.-.8.9.4.8.-.e.b.d.d.8.8.4.c.0.7.e.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.a.b.4.c.d.b.a.-.d.a.f.a.-.4.4.b.f.-.b.7.d.6.-.c.1.9.b.7.9.e.5.e.b.5.5.....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.=.B.a.n.k. .S.w.i.f.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.5.8.-.0.0.0.1.-.0.0.1.7.-.c.6.9.a.-.2.3.a.e.9.e.c.9.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.2.3.e.3.2.9.6.1.5.b.b.0.9.0.9.4.8.8.b.5.c.7.2.f.3.2.a.1.5.e.5.0.0.0.0.f.f.f.f.!.0.0.0.0.c.5.d.7.f.d.7.b.9.0.5.e.c.9.7.6.a.f.2.1.f.b.7.8.f.7.f.b.b.b.5.1.6.7.6.7.d.a.2.f.!.B.a.n.k. .S.w.i.f.t...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 3 18:04:04 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	18256
Entropy (8bit):	2.1674567117949786
Encrypted:	false
SSDEEP:	96:5cN8Q/dMR0cTm0LVosbHU1IbNhMiXpCdt12fylWInWIX4I4/560nnGA:sGacKZ1CvMMCdMyK/MsnGA
MD5:	13F1799F03A7AC23B94D4A5BF4B5DA79
SHA1:	5411C2FD439B32289C5C5F098B3F4F7B9EB633F0
SHA-256:	C2450E30D3F812B94D5D9EDF74CC8E9063305258925B33212ADF7A21680678B9
SHA-512:	90586ED4E7DC04A40FCD2FE238B75511C6C06FCA0FFA136DE71D1CD68A43AD014DBA96F9D02A6CBF3622866046EA600CEF0A922C3349AE55B74210391C182B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....(._.....U.....B.....GenuineIntelW.....T.....X....(._.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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):	8284
Entropy (8bit):	3.696183479397755
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVHL6TJ/9fC6YghSUZm2gmfXSQCprJ89bCngsf02m:RrlsNi9L699fC6YGSUZm2gmfXSOCnzf8
MD5:	1E3244F8DED4DEFD69A9D28898100BB1
SHA1:	55C50AE05E7F994FDC542F07616FFD6EF1C7C49A
SHA-256:	F2B6ED1C8EEF0BEDFFA701EBCAACC0F33CBA5E8E95FBCB0D6881E4986868FBFA
SHA-512:	7D7628E5765066C62EBD10D2249AD8217D331AF25715834773B2CC9BB9D7A41578565F6E4734412B5DCDD7172F4E19166C5B25B5797C76BC78E4A5DFC5C7B78
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	
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.>.4.6.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4566
Entropy (8bit):	4.449454483084036
Encrypted:	false
SSDEEP:	48:cvIwSD8zs2JgtWI9DjWSC8B18fm8M4JpYFa/V+q8QuYoJkwv6wLd:uITfMkSSNoJRVYYoOwv6wLd
MD5:	B2F80A7136344658E844048CED2DB972
SHA1:	1D1B6AE6734B2C4E02769F85D76EC81261ED0485
SHA-256:	617DD1B8B5152EC8682E17B28D583C07268A5C2E717C9051983F31D52095DF02
SHA-512:	29BFE8B3D4A28C0956F7D95D52ED4E8E389957AB71F3DCA353BEA66DDE5A7B367CAB8821C331A331F93F4BEA7AE71C56574F155300848045F9FC2EC348AA87A9
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="756194" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.306275307055633
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	Bank Swift.exe
File size:	633856
MD5:	2ace5c4532c77c014a02cc027d725d83
SHA1:	c5d7fd7b905ec976af21fb78f7fbbb516767da2f
SHA256:	53ae2502a9fed69821959a54927023f131c6e62ebc4611 9d86e2eaad60356827
SHA512:	0ea190a125f3c27c8ed6feb6533ec8904cf34faef62517fa3f70e528bbc21870637bef7236360f46e53e7cbeaf8cd5b646416c1029901dc150684ecd46a9457f
SSDEEP:	6144:Kd9vx8vk3Ouk2wlpF3W/FVvG1kRzfp6GaQdIaWBGswTPkg:Krx33OukZlpF32FVvGalh6GaQeGT9
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`_.....G.....X.....h.....@.....C.....

File Icon

Icon Hash:	da9aa9a256abcb65

Static PE Info

General

Entrypoint:	0x476800

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FC88CBA [Thu Dec 3 06:59:06 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
call 00007F9DF4AD2EA5h
pop edx
sub edx, 06h
push edx
mov ebx, dword ptr fs:[00000030h]
mov ebx, dword ptr [ebx+0Ch]
mov ebx, dword ptr [ebx+0Ch]
mov ebx, dword ptr [ebx]
or ebx, ebx
or ebx, ebx
mov ebx, dword ptr [ebx]
xchg ecx, ecx
mov eax, dword ptr [ebx+18h]
and ecx, ecx
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [eax+3Ch]
add eax, dword ptr [ebp-04h]
mov eax, dword ptr [eax+78h]
add eax, dword ptr [ebp-04h]
or ecx, ecx
or ecx, ecx
and eax, eax
mov ebx, dword ptr [eax+20h]
xchg edx, edx
add ebx, dword ptr [ebp-04h]
xchg ecx, ecx
mov ecx, dword ptr [eax+1Ch]
xchg ebx, ebx
nop
xchg edx, edx
and ecx, ecx
add ecx, dword ptr [ebp-04h]
mov edx, dword ptr [eax+24h]
and ecx, ecx
and ebx, FFFFFFFFh
xchg ebx, ebx
or ecx, ecx
add edx, dword ptr [ebp-04h]
xchg ebx, ebx
xchg ecx, ecx
push ecx
mov esi, dword ptr [ebx]
add esi, dword ptr [ebp-04h]
and edx, edx

Instruction
push edx
xchg ebx, ebx
nop
or ebx, ebx
or ebx, ebx
and ecx, ecx
push esi
and ecx, ecx
and edx, edx
and ecx, ecx
and edx, FFFFFFFFh
and ebx, ebx
call 00007F9DF4AD2F5Ah
and edx, edx
pop edx
cmp eax, 0038D13Ch
je 00007F9DF4AD2EB3h
add ebx, 04h
or ecx, ecx
add edx, 02h
jmp 00007F9DF4AD2E68h
pop ecx
xchg ebx, ebx
xchg edx, edx
and ebx, FFFFFFFFh
xchg ecx, ecx
xor ebx, ebx
and ecx, ecx
mov bx, word ptr [edx]
or ecx, ecx
imul ebx, ebx, 04h
mov eax, dword ptr [ecx+ebx]
and ebx, ebx
and eax, eax
add eax, dword ptr [ebp-04h]
or ecx, ecx
pop edx
and ebx, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x93000	0xadae	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x759ae	0x75a00	False	0.269228214665	PE32 executable (GUI) Intel 80386, for MS Windows	4.2724741752	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x77000	0x7b8	0x800	False	0.625	data	5.68691760105	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x78000	0x195f6	0x19600	False	0.956877309113	data	7.91626604629	IMAGE_SCN_MEM_READ
.tls	0x92000	0x7c	0x200	False	0.064453125	data	0.199775656087	IMAGE_SCN_MEM_READ
.rsrc	0x93000	0xadae	0xae00	False	0.539691091954	data	3.81210794401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x931a4	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x9370c	0x8a8	data		
RT_ICON	0x93fb4	0xea8	data		
RT_ICON	0x94e5c	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x96484	0x2ca8	data		
RT_ICON	0x9912c	0x4c28	dBase IV DBT, blocks size 0, block length 18432, next free block index 40, next free block 4241346293, next used block 1034317822		
RT_GROUP_ICON	0x9dd54	0x5a	data		

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:04:08.625196934 CET	63668	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:08.652194023 CET	53	63668	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:13.168123960 CET	54640	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:13.205226898 CET	53	54640	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:17.266319036 CET	58739	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:17.293328047 CET	53	58739	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:18.707664967 CET	60338	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:18.735018969 CET	53	60338	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:22.992645025 CET	58717	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:23.020464897 CET	53	58717	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:28.586172104 CET	59762	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:28.613363028 CET	53	59762	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:29.329097986 CET	54329	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:29.356168032 CET	53	54329	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:35.951611042 CET	58052	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:35.978822947 CET	53	58052	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:39.566442013 CET	54008	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:39.593497992 CET	53	54008	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:40.637523890 CET	59451	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:40.673032045 CET	53	59451	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:43.653302908 CET	52914	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:43.692128897 CET	53	52914	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:44.109178066 CET	64569	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:44.146260977 CET	53	64569	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:44.784944057 CET	52816	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:44.820770979 CET	53	52816	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:45.171366930 CET	50781	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:45.181185007 CET	54230	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:45.218492985 CET	53	50781	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:45.224344969 CET	53	54230	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:45.326652050 CET	54911	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:45.329180002 CET	49958	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:45.356254101 CET	53	49958	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:45.389111996 CET	53	54911	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:45.674350977 CET	50860	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:45.709924936 CET	53	50860	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:04:46.030839920 CET	50452	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:46.066523075 CET	53	50452	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:46.144993067 CET	59730	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:46.172111988 CET	53	59730	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:46.488519907 CET	59310	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:46.524024963 CET	53	59310	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:46.918834925 CET	51919	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:46.956573009 CET	53	51919	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:46.981966972 CET	64296	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:47.009016037 CET	53	64296	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:47.466274023 CET	56680	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:47.501998901 CET	53	56680	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:48.972369909 CET	58820	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:49.009903908 CET	53	58820	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:49.044904947 CET	60983	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:49.088216066 CET	53	60983	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:49.309803009 CET	49247	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:49.345410109 CET	53	49247	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:50.053294897 CET	52286	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:50.090537071 CET	53	52286	8.8.8.8	192.168.2.7
Dec 3, 2020 10:04:55.808554888 CET	56064	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:04:55.835467100 CET	53	56064	8.8.8.8	192.168.2.7
Dec 3, 2020 10:05:22.780018091 CET	63744	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:05:22.807009935 CET	53	63744	8.8.8.8	192.168.2.7
Dec 3, 2020 10:05:23.704996109 CET	61457	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:05:23.732042074 CET	53	61457	8.8.8.8	192.168.2.7
Dec 3, 2020 10:05:24.760817051 CET	58367	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:05:24.787975073 CET	53	58367	8.8.8.8	192.168.2.7
Dec 3, 2020 10:05:30.674300909 CET	60599	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:05:30.709754944 CET	53	60599	8.8.8.8	192.168.2.7
Dec 3, 2020 10:05:46.124448061 CET	59571	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:05:46.151633978 CET	53	59571	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:04.914928913 CET	52689	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:04.942213058 CET	53	52689	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:05.969528913 CET	50290	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:05.996619940 CET	53	50290	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:06.996464014 CET	60427	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:07.023490906 CET	53	60427	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:08.659492970 CET	56209	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:08.686654091 CET	53	56209	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:20.293653965 CET	59582	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:20.337250948 CET	53	59582	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:40.923434973 CET	60949	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:40.950665951 CET	53	60949	8.8.8.8	192.168.2.7
Dec 3, 2020 10:06:59.313481092 CET	58542	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:06:59.341099977 CET	53	58542	8.8.8.8	192.168.2.7
Dec 3, 2020 10:07:01.128875017 CET	59179	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:07:01.155968904 CET	53	59179	8.8.8.8	192.168.2.7
Dec 3, 2020 10:07:05.642198086 CET	60927	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:07:05.679966927 CET	53	60927	8.8.8.8	192.168.2.7
Dec 3, 2020 10:07:06.465666056 CET	57854	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:07:06.492929935 CET	53	57854	8.8.8.8	192.168.2.7
Dec 3, 2020 10:07:07.301096916 CET	62026	53	192.168.2.7	8.8.8.8
Dec 3, 2020 10:07:07.328151941 CET	53	62026	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:04:49.044904947 CET	192.168.2.7	8.8.8.8	0xed73	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:06:20.293653965 CET	192.168.2.7	8.8.8.8	0x541e	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

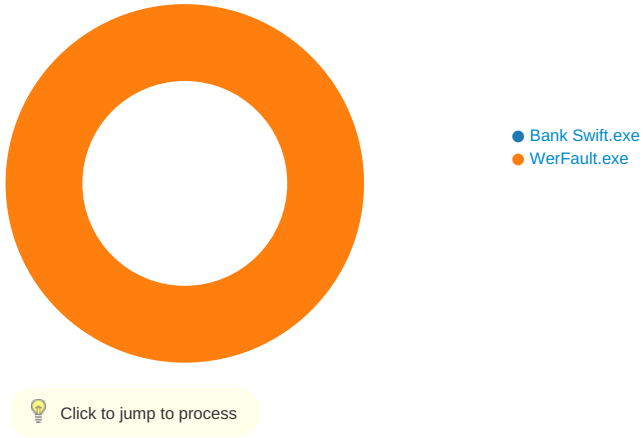
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:04:49.088216066 CET	8.8.8.8	192.168.2.7	0xed73	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:06:20.337250948 CET	8.8.8.8	192.168.2.7	0x541e	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Bank Swift.exe PID: 4696 Parent PID: 5648

General

Start time:	10:04:01
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\Bank Swift.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Bank Swift.exe'
Imagebase:	0x400000
File size:	633856 bytes
MD5 hash:	2ACE5C4532C77C014A02CC027D725D83
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 5488 Parent PID: 4696

General

Start time:	10:04:03
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4696 -s 216
Imagebase:	0xdf0000
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	6D8B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp.xml	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CD4.tmp.csv	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F84.tmp.txt	success or wait	1	6D8A497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 94 28 c9 5f a4 05 12 00 00 00 00 00	MDMP........ ....(._........	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.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 e0 0b 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 58 12 00 00 91 28 c9 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....X....(._.................. ....0..2............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.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 68 47 00 00 68 47 00 00 a0 22 00 00 68 47 00 00 68 47 00 9d 31 12 76 94 ff 0d 00 00 68 47 00 23 00 00 00 46 02 01 00 84 ff 0d 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+....hG..hG..."..hG..hG..1. v.....hG.#...F.......+.........	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	168	c0 13 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 68 47 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 9d 31 12 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 0c 00 00	.........................hG... ....1.v........ ....|...	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	20	06 00 00 00 48 b5 74 00 00 00 00 00 04 00 00 00 78 12 00 00	....H.t.........x...	success or wait	6	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	4	00 00 01 73	...s	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	256	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 68 47 00 00 68 47 00 00 00 00 00 18 f1 0d 00 bc 9a 30 77 23 00 00 00 06 02 00 00 88 ef 0d 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+................hG..hG..... ......0w#...........+.........	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	48	c0 13 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 d0 22 00 00 00 00 00 84 ef 0d 00 00 00 00 00 7c 10 00 00 14 28 00 00 cc 02 00 00 48 0f 00 00	....".............|.... (......H...	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	34	1c 00 00 00 42 00 61 00 6e 00 6b 00 20 00 53 00 77 00 69 00 66 00 74 00 2e 00 65 00 78 00 65 00 00 00	....B.a.n.k. .S.w.i.f.t...e.x.e...	success or wait	5	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	752	00 00 01 73 00 00 00 00 00 d0 09 00 8e f6 09 00 51 9e 0f b6 60 0c 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 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 f0 9a 02 00 00 00 00 00 20 e7 02 00 00 00 00 f7 43 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 09 29 03 00 00 00 00 00 be 5e 03 00 00 00 00 00 a6 2c 00 00 00 00 00 00 cd 81 1b 00 00 00 00 00 73 7d 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 de f9 0c 00 00 00 00	...s.....Q...`..... .....B.....B?..... .....$..... ..@A.....Zb..... .... .C.....).....^ .....,.....s}..... @.....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	3592	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 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4998.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 64 00 00 00 14 12 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 d0 08 00 00 c8 3e 00 00 15 00 00 00 ec 01 00 00 5c 09 00 00 16 00 00 00 98 00 00 00 48 0b 00 00	....4..... ...<.....d. .....T.....8..... ....T.....>..... ..\.....H...	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.6.9.6.<./.P.i.d.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 42 00 61 00 6e 00 6b 00 20 00 53 00 77 00 69 00 66 00 74 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.>.B.a.n.k. .S.w.i.f.t...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.2.4.2.<./.U.p.t.i.m.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 31 00 35 00 37 00 38 00 31 00 38 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.5.7.8.1.8.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 31 00 32 00 38 00 36 00 39 00 36 00 33 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.6.9.6.3.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	72	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 39 00 34 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.4.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 33 00 35 00 31 00 30 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.5.1.0.2.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 33 00 35 00 31 00 30 00 32 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.5.1.0.2.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.3.2.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.4.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 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.>.1.2.0.0.0.<./.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 31 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.>.1.1.7.2.8.<./.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 30 00 32 00 38 00 30 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.0.2.8.0.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 30 00 33 00 36 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.0.3.6.2.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 30 00 32 00 38 00 30 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.0.2.8.0.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 32 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.2.9.2.<./.P.i.d.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 35 00 37 00 34 00 31 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.5.7.4.1.4.<./.U.p.t.i.m.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 35 00 31 00 32 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.1.2.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 33 00 30 00 34 00 30 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.3.0.4.0.6.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 39 00 32 00 37 00 32 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.9.2.7.2.3.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 38 00 32 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.9.8.2.5.1.2.<./.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 33 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.3.4.0.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 38 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.>.7.2.8.8.0.<./.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 35 00 35 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.>.7.0.5.5.2.<./.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.9.5.1.1.6.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 39 00 34 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.7.9.4.3.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.9.5.1.1.6.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 42 00 61 00 6e 00 6b 00 20 00 53 00 77 00 69 00 66 00 74 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.>.B.a.n.k. .S.w.i.f.t...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 62 00 77 00 77 00 65 00 76 00 65 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.>.b.w.w.e.v.e.,. .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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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 62 00 77 00 77 00 65 00 76 00 65 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.>.b.w.w.e.v.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 30 00 37 00 37 00 39 00 36 00 38 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.0.7.7.9.6.8.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 33 00 54 00 31 00 38 00 3a 00 30 00 34 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.2.-.0.3.T.1.8.:.0.4.:.0.5.Z.".>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 36 00 39 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 37 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.5.". .P.I.D.=.".4.6.9.6.". .U.p.t.i.m.e.M.S.=.".3.7.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.7.5.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 62 00 64 00 30 00 61 00 34 00 39 00 62 00 2d 00 62 00 37 00 31 00 37 00 2d 00 34 00 38 00 36 00 30 00 2d 00 38 00 39 00 34 00 38 00 2d 00 65 00 62 00 64 00 64 00 38 00 38 00 34 00 63 00 30 00 37 00 65 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.b.d.0.a.4.9.b.-.b.7.1.7.-.4.8.6.0.-.8.9.4.8.-.e.b.d.d.8.8.4.c.0.7.e.b.<./.G.u.i.d.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 33 00 54 00 31 00 38 00 3a 00 30 00 34 00 3a 00 30 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.2.-.0.3.T.1.8.:.0.4.:.0.5.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF0.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	6D8A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB7.tmp.xml	unknown	4566	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	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379\Report.wer	unknown	2	ff fe	..	success or wait	1	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379\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	130	6D8A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1523d379\Report.wer	unknown	42	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 39 00 35 00 32 00 37 00 35 00 37 00 30 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.9.5.2.7.5.7.0.6.	success or wait	1	6D8A497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe\8e82ed97	success or wait	1	6D8C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D8C1FB2	RegCreateKeyExW
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe\8e82ed97	ProgramId	unicode	0006223e329615bb0909488b5c72f32a15e50000ffff	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe\8e82ed97	FileId	unicode	0000c5d7fd7b905ec976af21fb78f7fbbb516767da2f	success or wait	1	6D8C36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	LowerCaseLongPath	unicode	c:\users\user\desktop\bank swift.exe	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	LongPathHash	unicode	bank swift.exe|8e82ed97	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	Name	unicode	bank swift.exe	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	Publisher	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	Version	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	BinFileVersion	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	BinaryType	unicode	pe32_i386	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	ProductName	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	ProductVersion	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	LinkDate	unicode	12/03/2020 06:59:06	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	BinProductVersion	unicode		success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	Size	B	00 AC 09 00 00 00 00 00	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	Language	dword	0	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	IsPeFile	dword	1	success or wait	1	6D8C36BF	unknown
\REGISTRY\A\{a6ec6cf8-a1d6-7c12-8ce0-b881d37d1a02}\Root\InventoryApplicationFile\bank swift.exe|8e82ed97	IsOsComponent	dword	0	success or wait	1	6D8C36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 68 47 00 02 00 00 00 01 00 00 00 9D 31 12 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D8C1FE8	RegSetValueExW

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

Disassembly

Code Analysis