ID: 326331
Sample Name: Bank Swift.exe
Cookbook: default.jbs
Time: 09:57:46
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

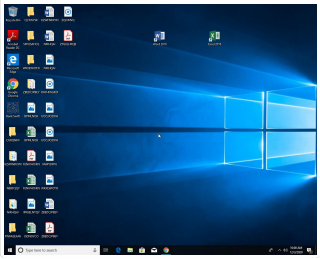
Analysis Report Bank Swift.exe

Overview

General Information

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

Most interesting Screenshot:



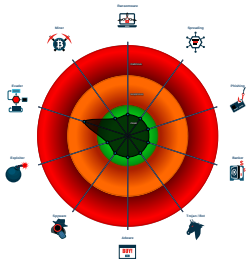
Detection

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…
- 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: 7028 cmdline: 'C:\Users\user\Desktop\Bank Swift.exe' MD5: 2ACE5C4532C77C014A02CC027D725D83)
  - WerFault.exe (PID: 7096 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7028 -s 216 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

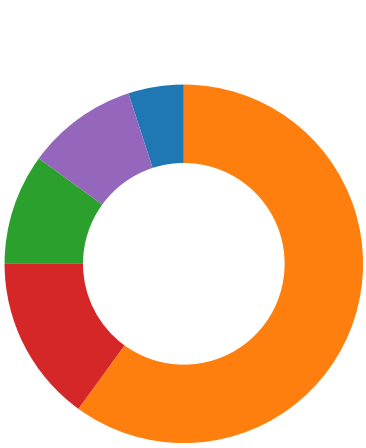
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

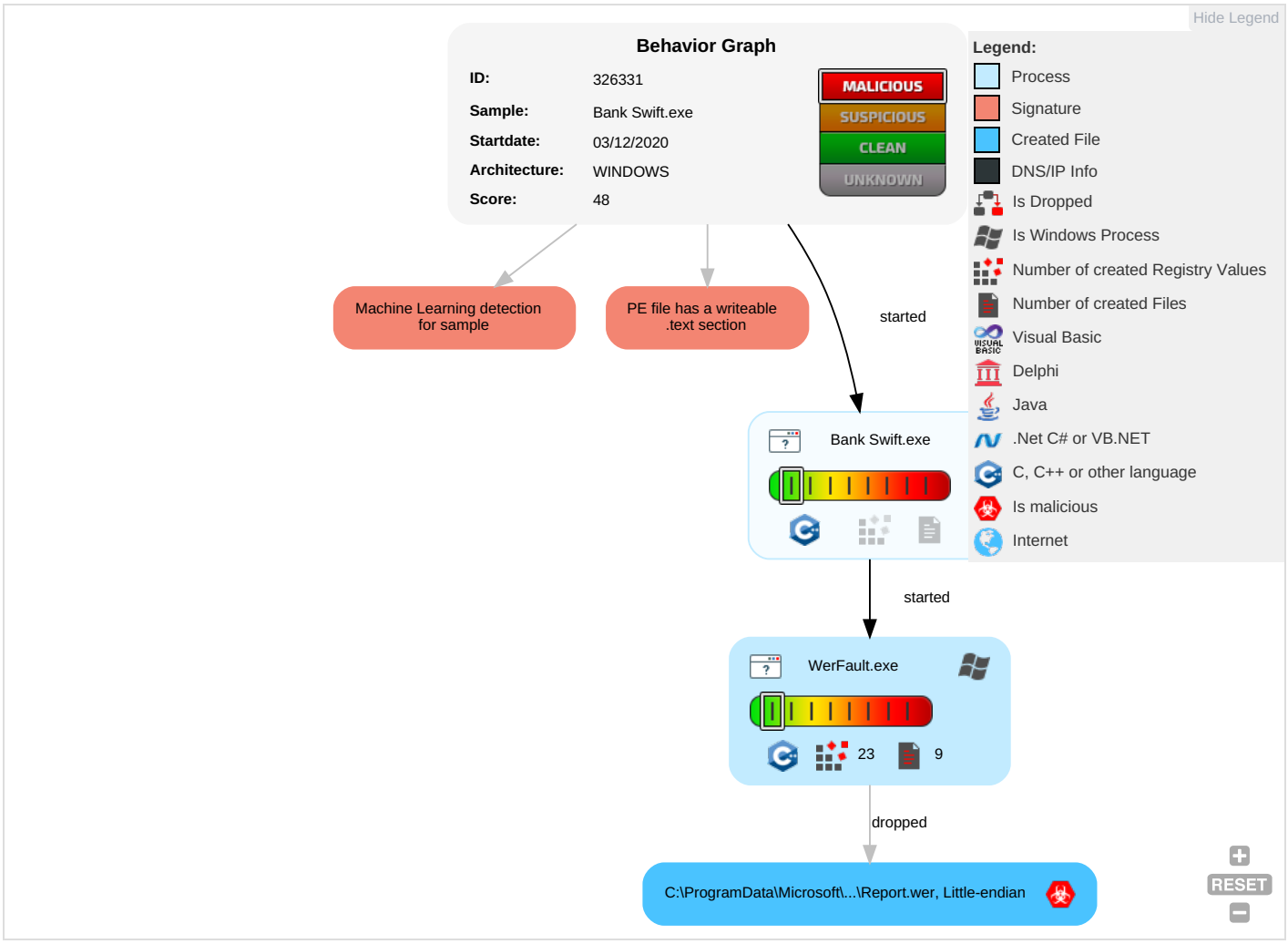
System Summary:

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	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	Junk Data	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	

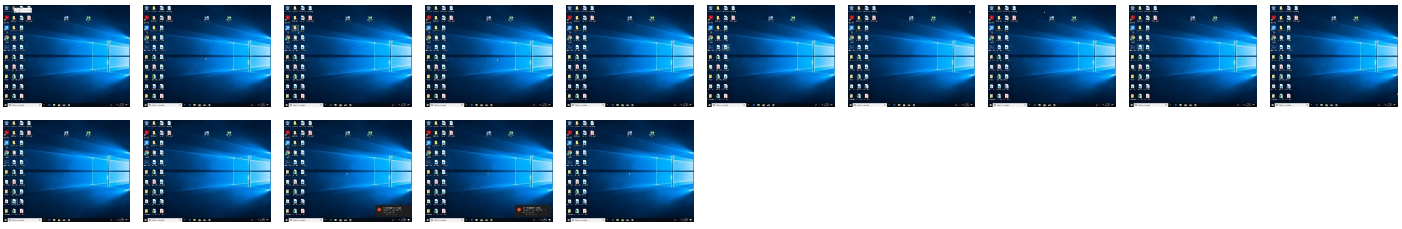
Behavior Graph



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

No contacted domains info

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:	09:57:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 29s
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
Number of analysed new started processes analysed:	19
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@0/0
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 • 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, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.43.139.144, 51.104.144.132, 104.42.151.234, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.103.5.159, 92.122.213.247, 92.122.213.194, 51.11.168.160, 92.122.144.200 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.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, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net

Simulations

Behavior and APIs

Time	Type	Description
09:58:55	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Bank Swift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7724
Entropy (8bit):	3.7592295138448635
Encrypted:	false
SSDEEP:	96:rUrWs7VUZAQEh8O75f0pXIQcQvc6QcEDMcw3DL+HbHg0c/NZAXGng5FMTPSkvPk3:wrhJUZAwHBUZMXojh/u7slS274Itwc
MD5:	A3062D7453C3D6CBA795C8E48515A971
SHA1:	2727FF3D64A74B85C3E6B34AF1620980C8A57101
SHA-256:	EE52CD117C41E0F3700BD787EB611A398EFE7EA6287790B2B0F01E51125F7E95
SHA-512:	074EAD4BE739ECD4D63163A3A2835A70F739645319DA8BE1E32477DB0B71022025F68BDDCE9565F24B2A56486888847E2E2E608D2AA20F2E10761094E7EBC521
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.=.1.3.2.5.1.4.9.1.9.2.1.9.2.1.7.1.4.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.1.4.9.1.9.2.4.9.2.1.7.0.5.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.0.1.c.6.e.5.b.-.7.2.9.3.-.4.e.1.7.-.9.b.f.8.-.9.f.2.0.e.e.a.0.3.c.f.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.3.c.3.3.6.9.e.-.8.3.6.e.-.4.5.b.0.-.b.1.7.a.-.4.a.5.2.2.d.2.0.7.d.c.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.b.7.4.-.0.0.0.1.-.0.0.1.7.-.a.e.3.0.-.c.a.e.d.9.d.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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 3 17:58:42 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	18256
Entropy (8bit):	2.159165985339814
Encrypted:	false
SSDEEP:	96:5HKs8Q/DhBUJC0JuhN1GE8gfCUrfn1bgkMiTpTQuLnJ+TxWInWIX4I4n5i/DnvA:4g1BUJC0JcNDC8RM8TTrJ+KnUbnvA
MD5:	D4556B67004A21DD871FEEC108AFC10C
SHA1:	318CA739D60B783DBC5DC3BB2DBB3EDB215896DB
SHA-256:	34AB0A4D1C243F9498928D4B6FDA1E77E63C6E8727F451D9F18F4CD59FC4823F
SHA-512:	78444B741A5240A32205A909631E27F3F7CD67E83DB4BCA066C194E14C1449C4C83C93277D2C4B2D602BD95A38D17E56176321AA42F2694A5B1E30A145B8FD61
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....R'._.....U.....B.....GenuineIntelW.....T.....t...O'._.....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\WER2114.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):	3.698943372303405
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFih6p0JQ9fC6YJdSUJd6EgmfXSaCprt89b/1sf08v1m:RrlsNish6Z9fC6YDSUJd6EgmfXS4/OfI
MD5:	E32E49AC580A06173092EEAD03451D4B
SHA1:	FEB773079E493A51F616B86F3C292CAE1B4EBC4C
SHA-256:	17DD8D365D235E2D8C7099D832AEF9E7136F01C84BC1B5EF66505BB0F87517C3
SHA-512:	39130C14E19A81DAC1B772A2349F4E4A340604A693008503961165911875D095B119A196699C1945646FAC02547570D856CDFDA5CDA4BBDAAEBF0756AE638BF8
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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.>.7.0.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.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):	4.455773285336386
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1iJgtWI9OAWSC8Bls8fm8M4JpYFM+q8QaoJkwv6wXQd:uITf6F5SNRJvUoOwv6wXQd
MD5:	6FF1BF1AB8ACFFDBF8871C01989AE3FC
SHA1:	03909BE42171A3778594162DC5934E05E57E8A67
SHA-256:	077EDE95E1BCFB4C4CB68F88DD91E845C9B9DB4B4A607149FD0B9C38E52D23DF
SHA-512:	664821FCD28F72F7E28B2531B3E34E2D9F492DCACE38D6D7D126338F9840EA0D083185C3B0425FC6A615D2C345DABB00B3437D8954D70F975607E99FD039B45
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="756189" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	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 d86e2eaad60356827
SHA512:	0ea190a125f3c27c8ed6feb6533ec8904cf34faef62517fa 3f70e528bbc21870637bef7236360f46e53e7cbeaf8cd5b 646416c1029901dc150684ecd46a9457f
SSDEEP:	6144:Kd9vx8vk3Ouk2wlpF3W/FVvG1kRzfp6GaQdIaW BGswTPkg: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
Entrypoint Section:	.text

General

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 00007FA85C74A155h
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
push edx

Instruction
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 00007FA85C74A20Ah
and edx, edx
pop edx
cmp eax, 0038D13Ch
je 00007FA85C74A163h
add ebx, 04h
or ecx, ecx
add edx, 02h
jmp 00007FA85C74A118h
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
.rdata	0x77000	0x7b8	0x800	False	0.625	data	5.68691760105	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

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

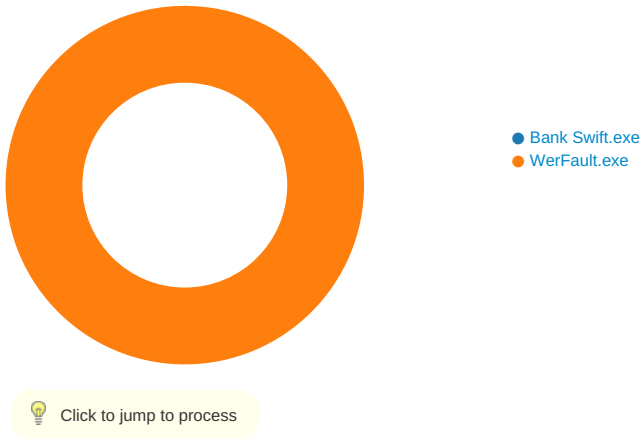
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:58:33.007957935 CET	54064	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:33.035159111 CET	53	54064	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:33.813399076 CET	52811	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:33.840426922 CET	53	52811	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:34.622200966 CET	55299	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:34.658046007 CET	53	55299	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:42.543369055 CET	63745	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:42.570534945 CET	53	63745	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:43.717699051 CET	50055	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:43.744678020 CET	53	50055	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:44.712975979 CET	61374	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:44.740035057 CET	53	61374	8.8.8.8	192.168.2.6
Dec 3, 2020 09:58:45.236205101 CET	50339	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:58:45.263329983 CET	53	50339	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:00.758932114 CET	63307	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:00.785965919 CET	53	63307	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:17.639456034 CET	49694	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:17.666378975 CET	53	49694	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:20.061356068 CET	54982	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:20.088129997 CET	53	54982	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:20.603008032 CET	50010	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:20.655071020 CET	53	50010	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:21.244880915 CET	63718	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:21.280440092 CET	53	63718	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:21.378500938 CET	62116	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:21.405493975 CET	53	62116	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:21.691581011 CET	63816	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:21.779614925 CET	53	63816	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.071378946 CET	55014	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.107191086 CET	53	55014	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.465591908 CET	62208	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.477787018 CET	57574	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.501205921 CET	53	62208	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.505228996 CET	53	57574	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.727617025 CET	51818	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.763194084 CET	53	51818	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.780606031 CET	56628	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.817647934 CET	53	56628	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:59:22.882082939 CET	60778	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.917150974 CET	53	60778	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:22.960058928 CET	53799	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:22.997616053 CET	53	53799	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:23.452016115 CET	54683	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:23.487421989 CET	53	54683	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:24.733033895 CET	59329	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:24.768492937 CET	53	59329	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:25.380677938 CET	64021	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:25.407536030 CET	53	64021	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:26.140074968 CET	56129	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:26.175757885 CET	53	56129	8.8.8.8	192.168.2.6
Dec 3, 2020 09:59:29.513184071 CET	58177	53	192.168.2.6	8.8.8.8
Dec 3, 2020 09:59:29.550185919 CET	53	58177	8.8.8.8	192.168.2.6
Dec 3, 2020 10:00:00.666518927 CET	50700	53	192.168.2.6	8.8.8.8
Dec 3, 2020 10:00:00.693614960 CET	53	50700	8.8.8.8	192.168.2.6
Dec 3, 2020 10:00:00.959947109 CET	54069	53	192.168.2.6	8.8.8.8
Dec 3, 2020 10:00:01.004128933 CET	53	54069	8.8.8.8	192.168.2.6
Dec 3, 2020 10:00:07.371217966 CET	61178	53	192.168.2.6	8.8.8.8
Dec 3, 2020 10:00:07.408102989 CET	53	61178	8.8.8.8	192.168.2.6
Dec 3, 2020 10:00:24.997495890 CET	57017	53	192.168.2.6	8.8.8.8
Dec 3, 2020 10:00:25.024599075 CET	53	57017	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Bank Swift.exe PID: 7028 Parent PID: 5800

General

Start time:	09:58:39

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: 7096 Parent PID: 7028

General

Start time:	09:58:40
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7028 -s 216
Imagebase:	0xd90000
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	6F3E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Bank Swift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F3D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F3D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.tmp	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	success or wait	1	6F3D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	success or wait	1	6F3D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.tmp.xml	success or wait	1	6F3D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2365.tmp.csv	success or wait	1	6F3D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2654.tmp.txt	success or wait	1	6F3D4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 52 27 c9 5f a4 05 12 00 00 00 00 00	MDMP........ ....R'._........	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.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 74 1b 00 00 4f 27 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 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... ....t...O'._................. ....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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.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 00 3d 00 00 68 47 00 00 68 47 00 28 9d ac 02 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	....+...S...+. ..+....hG..hG...=..hG..hG. (........hG.#...F.......+.........	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	168	78 1b 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 28 9d ac 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	x........................hG... ....(........... ....|...	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	20	06 00 00 00 00 00 3d 00 00 00 00 00 98 04 00 00 78 12 00 00	......=.........x...	success or wait	6	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	1176	00 00 00 00 ff ff ff ff 00 00 40 00 a0 7b f0 77 70 17 5b 00 00 00 00 00 00 00 5b 00 a0 79 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 f8 7b f0 77 01 00 01 00 00 00 00 00 00 00 eb 7f 00 00 00 00 30 07 eb 7f 00 00 fb 7f 28 02 fc 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 f0 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........@..{.wp.[.......[..y .w................................ {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	256	c2 08 00 90 b8 54 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 55 00 00 00 ba e0 dc e6 77 ff d2 c2 2c 00 90 b8 56 00 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 57 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 58 00 00 00 ba e0 dc e6 77 ff d2 c2 0c 00 90 b8 59 00 00 00 ba e0 dc e6 77 ff d2 c2 40 00 90 b8 5a 00 18 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 5b 00 1d 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 5c 00 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 5d 00 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 5e 00 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 5f 00 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 60 00 00 00 ba e0 dc e6 77 ff d2 c2 18 00 90 b8 61 00 07 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 62 00 00 00 ba e0 dc e6 77 ff d2 c2 1c 00 90 b8 63 00 00 00 ba e0 dc e6 77 ff	.....T.......w.......U.......w ...,...V.......w.......W...... .w.......X.......w.......Y.... ...w...@...Z.......w.......[.. .....w.......\.......w.......] ....w.......^.......w...... ._.......w.......`.......w.... ...a.......w.......b.......w.. .....c.......w.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 68 47 00 00 68 47 00 00 00 00 00 18 f1 0d 00 bc 9a e5 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 aa aa aa aa	?............................ ....+...S...+. ..+................hG..hG..... ....w#...........+.........	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	48	78 1b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 30 3d 00 00 00 00 00 84 ef 0d 00 00 00 00 00 7c 10 00 00 14 27 00 00 cc 02 00 00 48 0f 00 00	x....... ....0=.......... ..|....'......H...	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.tmp.dmp	unknown	752	00 00 b6 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 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 e0 b2 02 00 00 00 00 00 50 d0 02 00 00 00 00 e9 3f 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 b9 6c 03 00 00 00 00 00 97 71 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 eb 72 1b 00 00 00 00 00 55 8c 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00	...s.....Q...`..... .....B.....B?..... .....$..... ..@A.....Zb..... ....P..... .?.....I.....q .....r.....U..... @.....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.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 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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F7D.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.2.8.<./.P.i.d.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.2.4.<./.U.p.t.i.m.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.4.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.2.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.7.6.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 33 00 32 00 35 00 32 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.3.3.2.5.2.7.<./.U.p.t.i.m.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 32 00 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.8.2.9.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 37 00 35 00 38 00 31 00 34 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.>.1.0.6.7.5.8.1.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 36 00 34 00 32 00 36 00 33 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.4.2.6.3.6.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 37 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.1.7.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 37 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.7.8.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 35 00 34 00 34 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.>.7.5.4.4.0.<./.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 33 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.2.4.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 35 00 37 00 36 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.7.6.2.1.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 38 00 31 00 30 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.8.1.0.1.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 35 00 37 00 36 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.7.6.2.1.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 78 00 67 00 6a 00 75 00 71 00 6a 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.>.x.g.j.u.q.j.,. .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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 78 00 67 00 6a 00 75 00 71 00 6a 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.>.x.g.j.u.q.j.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 34 00 30 00 35 00 38 00 39 00 33 00 32 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.>.1.5.6.4.0.5.8.9.3.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 37 00 3a 00 35 00 38 00 3a 00 34 00 32 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.1.7.:.5.8.:.4.2.Z.".>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 34 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 32 00 38 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 34 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 34 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.=.".3.4.7.". .P.I.D.=.".7.0.2.8.". .U.p.t.i.m.e.M.S.=.".3.7.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.7.4.". .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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 30 00 31 00 63 00 36 00 65 00 35 00 62 00 2d 00 37 00 32 00 39 00 33 00 2d 00 34 00 65 00 31 00 37 00 2d 00 39 00 62 00 66 00 38 00 2d 00 39 00 66 00 32 00 30 00 65 00 65 00 61 00 30 00 33 00 63 00 66 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.0.1.c.6.e.5.b.-.7.2.9.3.-.4.e.1.7.-.9.b.f.8.-.9.f.2.0.e.e.a.0.3.c.f.4.<./.G.u.i.d.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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 37 00 3a 00 35 00 38 00 3a 00 34 00 32 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.1.7.:.5.8.:.4.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.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	6F3D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2338.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	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8\Report.wer	unknown	2	ff fe	..	success or wait	1	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8\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	134	6F3D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_BankSwift.exe_80879c17d1924b75c27e84dfcffed9edc11fd3_314a8f1f_1bfaced8\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 37 00 35 00 32 00 38 00 37 00 36 00 38 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.8.7.5.2.8.7.6.8.4.	success or wait	1	6F3D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	success or wait	1	6F3F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F3F1FB2	RegCreateKeyExW
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F3D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	ProgramId	unicode	0006223e329615bb0909488b5c72f32a15e50000ffff	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	FileId	unicode	0000c5d7fd7b905ec976af21fb78f7fbbb516767da2f	success or wait	1	6F3F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	LowerCaseLongPath	unicode	c:\users\user\desktop\bank swift.exe	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	LongPathHash	unicode	bank swift.exe|c8909815	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	Name	unicode	bank swift.exe	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	Publisher	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	Version	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	BinFileVersion	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	BinaryType	unicode	pe32_i386	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	ProductName	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	ProductVersion	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	LinkDate	unicode	12/03/2020 06:59:06	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	BinProductVersion	unicode		success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	Size	B	00 AC 09 00 00 00 00 00	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	Language	dword	0	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	IsPeFile	dword	1	success or wait	1	6F3F36BF	unknown
\REGISTRY\A\{bb6802ab-7f84-9ee3-45d9-ad5c35a4d977}\Root\InventoryApplicationFile\bank swift.exe|c8909815	IsOsComponent	dword	0	success or wait	1	6F3F36BF	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 28 9D AC 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6F3F1FE8	RegSetValueExW

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

Disassembly

Code Analysis