ID: 346431
Sample Name: jesovROZ8A
Cookbook: default.jbs
Time: 15:48:11
Date: 31/01/2021
Version: 31.0.0 Emerald

Table of Contents

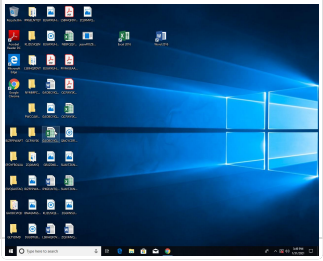
Analysis Report jesovROZ8A

Overview

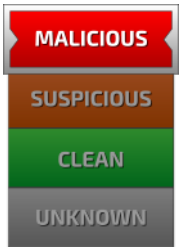
General Information

Sample Name:	jesovROZ8A (renamed file extension from none to exe)
Analysis ID:	346431
MD5:	039ce25d495fa55.
SHA1:	6684d0ffde17405..
SHA256:	94fff127753ed1d…
Tags:	unnamed3

Most interesting Screenshot:



Detection

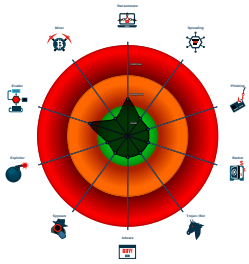


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Detected potential crypto function
- One or more processes crash
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- jesovROZ8A.exe (PID: 6760 cmdline: 'C:\Users\user\Desktop\jesovROZ8A.exe' MD5: 039CE25D495FA555AE1C210592B564D0)
  - WerFault.exe (PID: 6820 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6760 -s 588 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

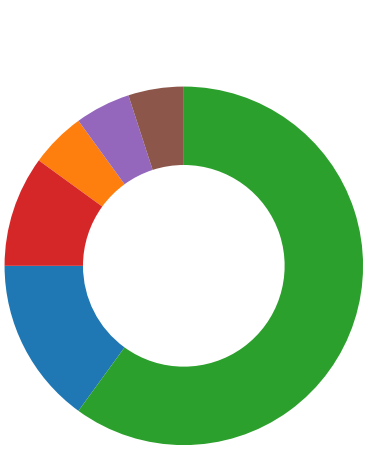
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

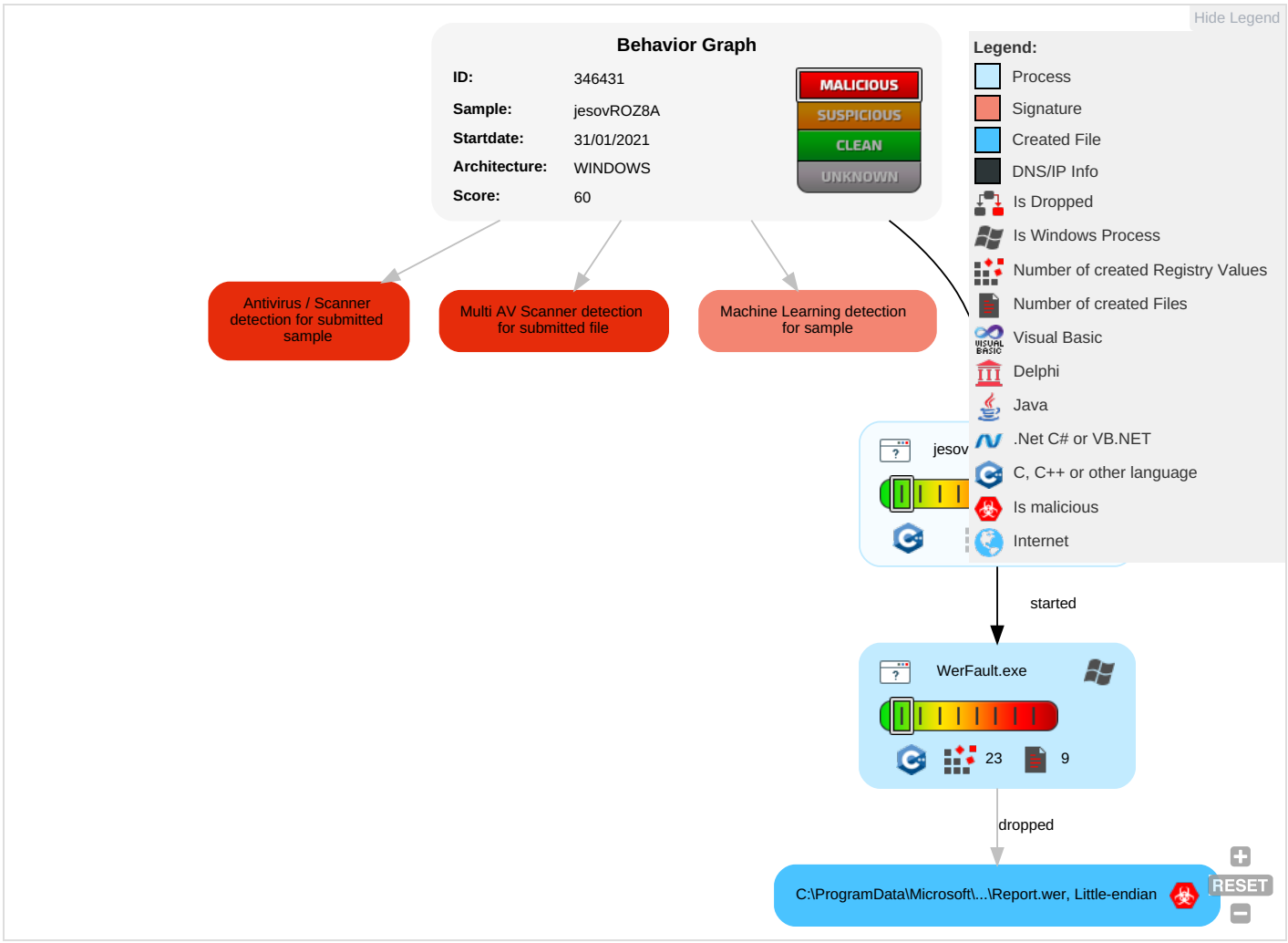
Compliance:

Uses 32bit PE files

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

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
jesovROZ8A.exe	86%	Virustotal		Browse
jesovROZ8A.exe	100%	ReversingLabs	Win32.Trojan.Zeus	
jesovROZ8A.exe	100%	Avira	TR/Sirefef.AO	
jesovROZ8A.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.jesovROZ8A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.jesovROZ8A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346431
Start date:	31.01.2021
Start time:	15:48:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jesovROZ8A (renamed file extension from none to 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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winEXE@2/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.3% (good quality ratio 69.2%) • Quality average: 47% • Quality standard deviation: 34.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): WerFault.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 13.88.21.125 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

Time	Type	Description
15:48:59	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_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11736
Entropy (8bit):	3.7735213884049688
Encrypted:	false
SSDEEP:	192:detqH/8yKjHBUZMXYjdKV//u7sOS274ltDXs:lH/8y+BUZMXYjM/u7sOX4ltDXs
MD5:	1F9065E7408B870CE000895D72BE6A22
SHA1:	0731D48C9E06AAE9C2C741D4AFAFD8F93B8E9257
SHA-256:	BB16FA02BECA9949F44A76A51E9DD2437455DEE884D5DCF1B581AA1500869FE3
SHA-512:	401D96BE2B1D6E8C24A018F0F01498848EC954D28F8588947B948A9D87D4322684E2C56E4AADED71C5CF3B3B4906C710966BC6DA0964D6C369EC823DF8CC2E
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.=.1.3.2.5.6.6.1.0.5.3.7.2.6.9.1.3.8.4.....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.=.1.3.2.5.6.6.1.0.5.3.7.9.7.2.2.6.0.3.....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.=.1.1.6.9.b.2.f.d.-.5.e.3.3.-.4.2.d.5.-.b.a.6.1.-.8.e.2.8.8.8.d.f.d.f.f.f.....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.=.d.7.9.4.8.7.1.9.-.3.3.c.2.-.4.e.f.d.-.a.4.e.5.-.8.a.a.c.f.0.4.0.c.5.e.1.....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.=.j.e.s.o.v.R.O.Z.8.A...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.C.h.e.v.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.6.8.-.0.0.0.1.-.0.0.1.7.-.8.a.2.6.-.d.2.a.2.2.b.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.e.9.9.7.4.9.2.3.7.a.0.6.0.7.c.4.b.f.6.b.d.7.1.4.a.8.4.d.c.b.3.0.0.0.0.0.9.0.4.!.0.0.0.0.6.6.8.4.d.0.f.f.d.e.1.7.4.0.5.2.a.0.3.9.3.1.9.8.1.2.6.2.d.c.0.a.7.c.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Jan 31 23:48:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47426
Entropy (8bit):	2.2142712366005073
Encrypted:	false
SSDEEP:	192:aIgGguASAaeMREMvIeWYxbsxzrpAkY2gA2wa7BU1a1RAf82Dik8lYF1:ouASuM/vWYxbsx3px1p2Bia1v2DikX1

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	
MD5:	52730B8719E5E6ADA0DDD23137DB1025
SHA1:	D77EB63F64A52355BD6367543D4BE03D473A952C
SHA-256:	B5C0EA4849E308E885601FBD5CA80B9950DF9AC1A034234E3B3E4C13FD242FBD
SHA-512:	E73263BF26B27042762A14EB4E1D3A46684DE6B2AAD57AB6529B7CBED768F5B5ACE4DEE17210EBAEB0E893998CE84E13AC95F636956E4D292C9C63065521FC9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....A.`.....U.....B.....GenuineIntelW.....T.....h....A.`.....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\WERF6DC.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):	3.697242777046635
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitk6oB6YSeSUtDSXgmfPjSE+CprR889b/usfo1m:RrlsNiu6O6YbSUtDqgmfPjScp/tfn
MD5:	253C880FCCD1BF88B0F083950A8096F8
SHA1:	9A177F3B2F9D6BA34F503D0F7B2DBC42AC436FD0
SHA-256:	F29C38900CEA01AC63940684272EEE69631131A20A1B6BA4F15302D1B8EADF01
SHA-512:	A581C2992AB4F8F1E222236A02784B833B851095C5D73EF2D5BC0B6297DDE0100012129380B86CC2D87B42AC8E9AC6698588D69A684F1348DCD4D11A0B8F36F
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...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.>.6.7.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.460278992789587
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9icWSC8BU8fm8M4JosSF8+q8qrNP9M0hpd:uITfjVVSNfJP1P9MCpd
MD5:	7AB859FAC8A6073B41D1278803874FE3
SHA1:	D21F3474E448E6487C03D907BCFCD690B1F88BC5
SHA-256:	0E0E5DC3F8274CFF34F98D4B29842A0E8BFA685507CF1083692FFF98AB8A12F1
SHA-512:	85BF87601753F3B2B07D81343906660F57227E940895AD4C4DF880204491EEF31D61E676AC9DDD04BEAF36D60A695BBCF9DB16DEF8085EBE4FC5557A4FC203F
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="841499" />.. <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, UPX compressed
Entropy (8bit):	7.9178862272744785

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.39% • UPX compressed Win32 Executable (30571/9) 0.30% • Win32 EXE Yoda's Crypter (26571/9) 0.26% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	jesovROZ8A.exe
File size:	202240
MD5:	039ce25d495fa555ae1c210592b564d0
SHA1:	6684d0ffde174052a03931981262dc0a7cb9891c
SHA256:	94fff127753ed1d704c781b5c391f5e62f4a907b67f7e1d51c3c84addd5851ab
SHA512:	c2be8d6b80e57339957f370b4ac31bd03140f9a9ed4865926eb6d7e5a69d3510b046930c1933d38629b4c3bcae007b6cf5e6140463ab6e064820cdd91bbd46bb
SSDEEP:	3072:RD9PfpJ/v2bIfdjba+htCsw0qv2AYjGX9E7e+q8EOADhpsWgXDeet78Bx/rUyMHL:RXJWbUTwsTqvdMO9nnSmphgTeE4B+8U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F...'...'...'.....h%.....;'...k...'..0...C'...y...&..<&...%.....&..^....%...w...&...3...$.....$...7..Z&..Rich.'.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x445590
Entrypoint Section:	UPX1
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:	0x4D771DAA [Wed Mar 9 06:26:50 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	8
OS Version Minor:	2
File Version Major:	8
File Version Minor:	2
Subsystem Version Major:	8
Subsystem Version Minor:	2
Import Hash:	976c9384d1a3c367e491662f20af4316

Entrypoint Preview

Instruction
pushad
mov esi, 00416000h
lea edi, dword ptr [esi-00015000h]
push edi
jmp 00007F6AFC7A0E6Dh
nop
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007F6AFC7A0E69h
mov ebx, dword ptr [esi]

Instruction
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F6AFC7A0E4Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F6AFC7A0E69h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F6AFC7A0E51h
jne 00007F6AFC7A0E6Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F6AFC7A0E46h
xor ecx, ecx
sub eax, 03h
jc 00007F6AFC7A0E6Fh
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F6AFC7A0ED6h
mov ebp, eax
add ebx, ebx
jne 00007F6AFC7A0E69h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jne 00007F6AFC7A0E69h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jne 00007F6AFC7A0E82h
inc ecx
add ebx, ebx
jne 00007F6AFC7A0E69h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F6AFC7A0E51h
jne 00007F6AFC7A0E6Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F6AFC7A0E46h
add ecx, 02h
cmp ebp, FFFFF300h
adc ecx, 01h
lea edx, dword ptr [edi+ebp]
cmp ebp, FFFFFFFCh
jbe 00007F6AFC7A0E71h
mov al, byte ptr [edx]
inc edx
mov byte ptr [edi], al
inc edi
dec ecx

Instruction
jne 00007F6AFC7A0E59h
jmp 00007F6AFC7A0DC8h
nop
mov eax, dword ptr [edx]
add edx, 04h
mov dword ptr [edi], eax
add edi, 04h
sub ecx, 04h
jnbe 00007F6AFC7A0E53h
add edi, ecx
jmp 00007F6AFC7B0DB1h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4749c	0x428	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x46000	0x149c	.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
UPX0	0x1000	0x15000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x16000	0x30000	0x2f800	False	0.996900699013	data	7.94664222533	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x2000	0x1a00	False	0.621394230769	data	5.74902503533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_FONT	0x463ec	0x5	data	English	United States
RT_FONT	0x463f8	0x5	data	English	United States
RT_FONT	0x46404	0x5	data	English	United States
RT_FONT	0x46410	0x5	data	English	United States
RT_FONT	0x4641c	0x5	data	English	United States
RT_FONT	0x46428	0x5	data	English	United States
RT_FONT	0x46434	0x5	data	English	United States
RT_FONT	0x46440	0x5	data	English	United States
RT_FONT	0x4644c	0x5	data	English	United States
RT_RCDATA	0x46458	0xb08	data	English	United States
RT_VERSION	0x46f64	0x32c	data	English	United States
RT_MANIFEST	0x47294	0x1be	ASCII text, with CRLF line terminators	English	United States
None	0x47458	0x5	data	English	United States
None	0x47464	0x5	Non-ISO extended-ASCII text, with no line terminators	English	United States
None	0x47470	0x5	data	English	United States
None	0x4747c	0x5	data	English	United States
None	0x47488	0x5	data	English	United States
None	0x47494	0x5	data	English	United States

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess
advapi32.dll	RegEnumKeyW
comctl32.dll	ImageList_Add
comdlg32.dll	ChooseColorW
crypt32.dll	CryptProtectData
gdi32.dll	DPtoLP
msimg32.dll	AlphaBlend
msvcrt.dll	exit
ole32.dll	DoDragDrop
rpcrt4.dll	UuidEqual
secur32.dll	GetUserNameExW
shell32.dll	ShellAboutW
shlwapi.dll	UrlIsW
urlmon.dll	CreateAsyncBindCtx
user32.dll	GetDC
version.dll	VerQueryValueW
wininet.dll	InternetOpenW
winmm.dll	mixerOpen

Version Infos

Description	Data
LegalCopyright	Crops Mama Poll 2003-2010
InternalName	Firm Veal Pores Funds Elms
FileVersion	8.9
CompanyName	Foundstone Inc.
ProductName	Yak Press Bent Met Shuts Cogent
ProductVersion	8.9
FileDescription	Wrong Knot Wilt Alto Shrew Strap
OriginalFilename	Chevy.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

UDP Packets

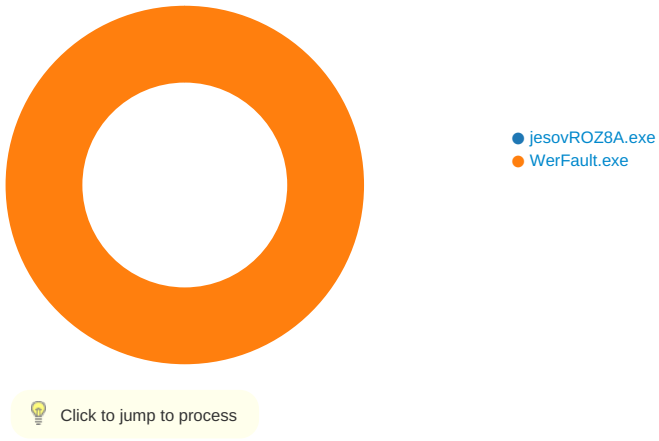
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2021 15:48:51.427562952 CET	53195	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:51.486624002 CET	53	53195	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:52.618102074 CET	50141	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:52.669011116 CET	53	50141	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:53.823244095 CET	53023	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:53.871365070 CET	53	53023	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:55.231226921 CET	49563	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:55.279221058 CET	53	49563	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:56.441545963 CET	51352	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:56.489640951 CET	53	51352	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:57.840215921 CET	59349	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:57.891206980 CET	53	59349	8.8.8.8	192.168.2.3
Jan 31, 2021 15:48:59.063894033 CET	57084	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:59.113573074 CET	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2021 15:48:59.712811947 CET	58823	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:48:59.775988102 CET	53	58823	8.8.8.8	192.168.2.3
Jan 31, 2021 15:49:01.016613007 CET	57568	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:49:01.064748049 CET	53	57568	8.8.8.8	192.168.2.3
Jan 31, 2021 15:49:02.666138887 CET	50540	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:49:02.719952106 CET	53	50540	8.8.8.8	192.168.2.3
Jan 31, 2021 15:49:03.982455015 CET	54366	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:49:04.032974958 CET	53	54366	8.8.8.8	192.168.2.3
Jan 31, 2021 15:49:05.172704935 CET	53034	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:49:05.223520994 CET	53	53034	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: jesovROZ8A.exe PID: 6760 Parent PID: 5912

General

Start time:	15:48:55
Start date:	31/01/2021
Path:	C:\Users\user\Desktop\jesovROZ8A.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\jesovROZ8A.exe'
Imagebase:	0x400000
File size:	202240 bytes
MD5 hash:	039CE25D495FA555AE1C210592B564D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 6820 Parent PID: 6760

General

Start time:	15:48:56
Start date:	31/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6760 -s 588
Imagebase:	0xfe0000
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	6E041717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E03497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp.xml	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E18.tmp.csv	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E29.tmp.txt	success or wait	1	6E034BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 e9 41 17 60 a4 05 12 00 00 00 00 00	MDMP........ ....A.`........	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.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 0c 1c 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 68 1a 00 00 e7 41 17 60 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 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....h....A.`................. ....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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.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 d4 f5 19 00 9b df 19 ff 06 00 74 08 00 00 00 00 01 00 00 00 30 d6 e6 77 80 ff 19 00 4b d6 e6 77 23 00 00 00 02 02 01 00 b4 f5 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.............t.........0..w ....K..w#...........+.........	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	168	6c 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 4b d6 e6 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9b df 19 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 e2 20 00 00	l......................K..w..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	20	15 00 00 00 c4 fd 97 00 00 00 00 00 3c 02 00 00 32 30 00 00	...........<...20..	success or wait	21	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe 97 00 24 ff 97 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 20 31 00 00 20 31 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 20 31 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa d8 d4 68 00 00 00 00 00 00 00 00 00 18 5e 68 00 00 90 30 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe a7 00 90 fe 87 00 98 fe a7 00 98 fe 87 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w............X...$..... ..@..w@..w..... 1.. 1......... .... 1.............. ....h... ....^h...0................	success or wait	20	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	6732	bc 9a e5 77 a3 1a 21 75 aa aa aa aa e8 e7 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 48 02 00 00 04 01 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 90 30 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 e7 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..!u...................... ......H...........$........... .... 0.............................	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 48 e7 19 00 bc 9a e5 77 23 00 00 00 06 02 00 00 b8 e5 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... H......w#...........+.........	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	48	78 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 31 00 00 00 00 00 c4 fd a7 00 00 00 00 00 3c 02 00 00 66 7c 00 00 cc 02 00 00 12 2c 00 00	x....... ....P1............ <...f|.......,..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	4	2a 00 00 00	*...	success or wait	42	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	34	1c 00 00 00 6a 00 65 00 73 00 6f 00 76 00 52 00 4f 00 5a 00 38 00 41 00 2e 00 65 00 78 00 65 00 00 00	....j.e.s.o.v.R.O.Z.8.A...e.x.e...	success or wait	42	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	752	00 00 a3 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 f4 0e ca 20 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 00 04 00 00 00 00 e0 9a 02 00 00 00 00 00 a0 c1 02 00 00 00 00 26 25 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 e3 56 03 00 00 00 00 00 a0 59 03 00 00 00 00 00 00 00 00 00 00 00 00 00 6b 89 1b 00 00 00 00 00 d5 75 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 78 ec 04 00 00 00 00	...t.....`..A!..-a... ....B.....B?..... .....#..... ..@A.....Zb..... .... &%.....V.....Y .....k.....u..... @.....x.....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	8348	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4E7.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 bc 11 00 00 cc 07 00 00 05 00 00 00 54 01 00 00 de 2e 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 80 17 00 00 0a a2 00 00 15 00 00 00 ec 01 00 00 88 19 00 00 16 00 00 00 98 00 00 00 74 1b 00 00	.....T. .....T.....8..... ....T..... .....t...	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.7.6.0.<./.P.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 6a 00 65 00 73 00 6f 00 76 00 52 00 4f 00 5a 00 38 00 41 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.>.j.e.s.o.v.R.O.Z.8.A...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 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	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 37 00 31 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.>.2.4.7.1.<./.U.p.t.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 39 00 32 00 34 00 36 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.2.4.6.7.2.0.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 39 00 31 00 39 00 35 00 31 00 31 00 30 00 34 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.>.9.1.9.5.1.1.0.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 31 00 35 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.>.2.0.1.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 37 00 37 00 33 00 37 00 33 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.>.7.7.3.7.3.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 37 00 37 00 33 00 37 00 33 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.7.3.7.3.4.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.4.9.6.0.<./.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.3.7.8.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.3.3.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 32 00 34 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.0.6.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 32 00 31 00 30 00 39 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.1.0.9.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 32 00 31 00 31 00 37 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.1.1.7.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 32 00 31 00 30 00 39 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.1.0.9.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 34 00 31 00 38 00 35 00 32 00 31 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.>.6.4.1.8.5.2.1.<./.U.p.t.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 30 00 35 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.>.4.8.0.5.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 34 00 38 00 37 00 38 00 30 00 38 00 30 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.>.1.0.4.8.7.8.0.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 35 00 34 00 32 00 32 00 30 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.>.1.0.4.5.4.2.2.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 36 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.6.5.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 31 00 34 00 33 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.>.9.3.1.4.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 33 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.7.4.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 33 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.0.3.1.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 39 00 30 00 31 00 34 00 34 00 30 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.>.3.5.9.0.1.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 38 00 30 00 33 00 31 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.0.3.1.3.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 39 00 30 00 31 00 34 00 34 00 30 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.>.3.5.9.0.1.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 6a 00 65 00 73 00 6f 00 76 00 52 00 4f 00 5a 00 38 00 41 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.>.j.e.s.o.v.R.O.Z.8.A...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 6e 00 73 00 6c 00 76 00 63 00 6b 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.>.n.s.l.v.c.k.,. .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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 6e 00 73 00 6c 00 76 00 63 00 6b 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.>.n.s.l.v.c.k.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 34 00 31 00 31 00 32 00 36 00 34 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.4.1.1.2.6.4.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 33 00 31 00 54 00 32 00 33 00 3a 00 34 00 38 00 3a 00 35 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.3.1.T.2.3.:.4.8.:.5.7.Z.".>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 35 00 39 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 35 00 39 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.=.".3.4.6.". .P.I.D.=.".6.7.6.0.". .U.p.t.i.m.e.M.S.=.".3.5.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.5.9.". .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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 31 00 36 00 39 00 62 00 32 00 66 00 64 00 2d 00 35 00 65 00 33 00 33 00 2d 00 34 00 32 00 64 00 35 00 2d 00 62 00 61 00 36 00 31 00 2d 00 38 00 65 00 32 00 38 00 38 00 38 00 64 00 66 00 64 00 66 00 66 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.1.6.9.b.2.f.d.-.5.e.3.3.-.4.2.d.5.-.b.a.6.1.-.8.e.2.8.8.8.d.f.d.f.f.f.<./.G.u.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 33 00 31 00 54 00 32 00 33 00 3a 00 34 00 38 00 3a 00 35 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.3.1.T.2.3.:.4.8.:.5.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6DC.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	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF74A.tmp.xml	unknown	4622	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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab\Report.wer	unknown	2	ff fe	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab\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	173	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_1ac5feab\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 32 00 34 00 32 00 31 00 34 00 33 00 31 00 39 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.2.4.2.1.4.3.1.9.5.	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	success or wait	1	6E0536BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E051FB2	RegCreateKeyExW
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0343D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	ProgramId	unicode	00063e99749237a0607c4bf6bd714a84dcb300000904	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	FileId	unicode	00006684d0ffde174052a03931981262dc0a7cb9891c	success or wait	1	6E0536BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	LowerCaseLongPath	unicode	c:\users\user\desktop\jesovroz8a.exe	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	LongPathHash	unicode	jesovroz8a.exe|70a5129d	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	Name	unicode	jesovroz8a.exe	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	Publisher	unicode	foundstone inc.	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	Version	unicode	8.9	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	BinFileVersion	unicode	8.9.0.0	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	BinaryType	unicode	pe32_i386	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	ProductName	unicode	yak press bent met shuts cogent	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	ProductVersion	unicode	8.9	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	LinkDate	unicode	03/09/2011 06:26:50	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	BinProductVersion	unicode	8.9.0.0	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	Size	B	00 16 03 00 00 00 00 00	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	Language	dword	1033	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	IsPeFile	dword	1	success or wait	1	6E0536BF	unknown
\REGISTRY\A\{fc61351e-8f50-970f-7088-9e478829e0b9}\Root\InventoryApplicationFile\jesovroz8a.exe|70a5129d	IsOsComponent	dword	0	success or wait	1	6E0536BF	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 4B D6 E6 77 02 00 00 00 00 00 00 00 9B DF 19 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E051FE8	RegSetValueExW

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

Disassembly

Code Analysis