ID: 326327
Sample Name: CUSTOM SHIPING DOCS.exe
Cookbook: default.jbs
Time: 09:59:38
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report CUSTOM SHIPING DOCS.exe

Overview

General Information

Sample Name:	CUSTOM SHIPING DOCS.exe
Analysis ID:	326327
MD5:	5533ec4c49c29a…
SHA1:	f3aa3401d15d44d…
SHA256:	ed8bdc7dfb03c55…
Tags:	exe

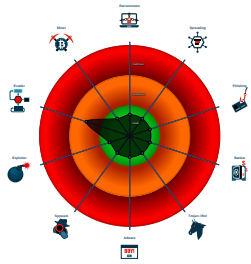
Detection

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

Signatures

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

Classification



Startup

- **System is w10x64**
- CUSTOM SHIPING DOCS.exe (PID: 4856 cmdline: 'C:\Users\user\Desktop\CUSTOM SHIPING DOCS.exe' MD5: 5533EC4C49C29A1225D1B01D38933BD4)
  - WerFault.exe (PID: 6088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4856 -s 216 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

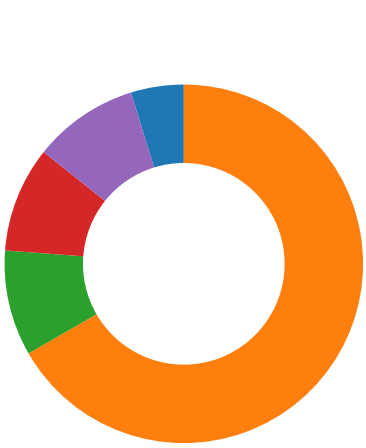
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Machine Learning detection for sample

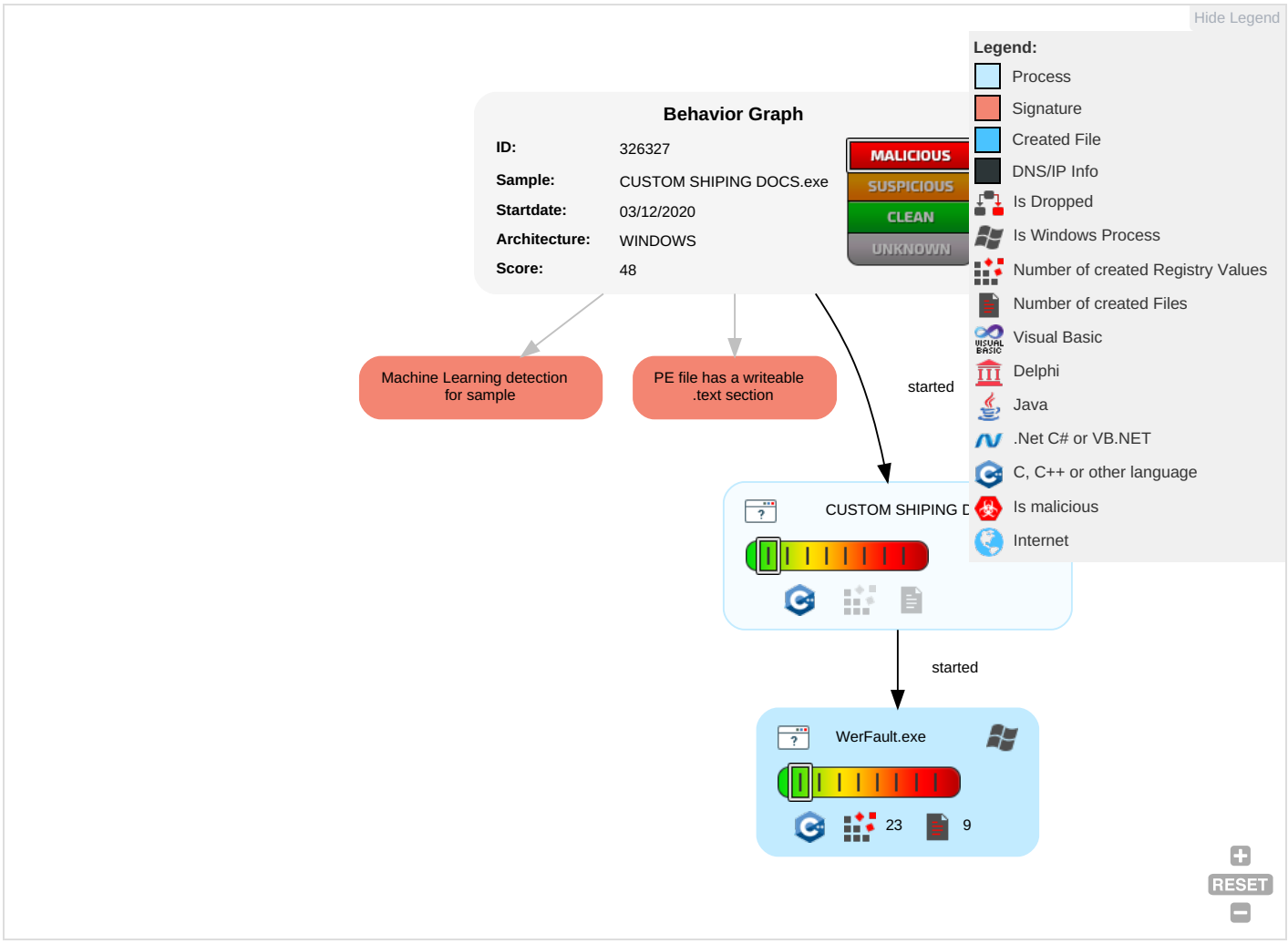
System Summary:

PE file has a writeable .text section

Mitre Att&ck Matrix

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

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CUSTOM SHIPING DOCS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326327
Start date:	03.12.2020
Start time:	09:59:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CUSTOM SHIPING DOCS.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winEXE@2/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): WerFault.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOM SHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7902
Entropy (8bit):	3.788331113066621
Encrypted:	false
SSDEEP:	192:d7C4jYzDVKGAbHBUZMXRsVjh/u7saS274ItMxL+U:BjcZSBUZMX4jh/u7saX4Itk+U
MD5:	C2BB5C169FE09D872650E12637929F14
SHA1:	4A3AAE485028B8626D3BA76D11584353787C0230
SHA-256:	355BA59F9FA3F5420BA2662B3CE2CCACD7CB4C52D44E701913631C320341FE68
SHA-512:	CAA5548F07FB1710EBCBE16C0F73B4217B573312BC2B5870EA8616F250EAA5F50FB55CD10FD8B43E43A1BC88580C2AFD6048068AF99DB3AF57E7325495326F7
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.1.4.9.2.0.3.3.9.4.8.3.2.3.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.1.4.9.2.0.3.4.6.0.4.5.6.2.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.f.4.5.3.d.6.8.-.5.a.2.4.-.4.e.4.d.-.9.e.f.3.-.d.7.5.8.4.6.f.8.b.c.5.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.0.8.4.7.4.5.0.-.9.8.c.b.-.4.f.6.b.-.a.d.8.0.-.0.5.e.1.b.c.9.5.8.f.4.1.....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.=.C.U.S.T.O.M. .S.H.I.P.I.N.G. .D.O.C.S...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.f.8.-.0.0.0.1.-.0.0.1.7.-.c.3.f.1.-.0.4.3.1.9.e.c.9.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.4.3.2.4.a.e.7.c.4.7.7.6.a.8.e.7.9.6.c.3.8.d.a.6.3.f.4.0.4.c.5.0.0.0.0.f.f.f.f.!.0.0.0.0.f.3.a.a.3.4.0.1.d.1.5.d.4.4.d.6.5.1.7.7.b.a.0.2.2.4.4.c.1.8.9.e.e.1.e.8.2.2.f.b.!.C.U.S.T.O.M. .S.H.I.P.I.N.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 3 18:00:34 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	18274
Entropy (8bit):	2.1773832169366063
Encrypted:	false
SSDEEP:	96:53m8Q/UqA1hC06u2i1GE8MOXfn57NQXi7oV+V+A5WInWIX4l49pQLyA:wBA1hC06ri2JNQXGoQO9pQLyA
MD5:	10465FC9B9CBB7D1B7E4261DDC1BE3AC
SHA1:	4CFABC8E3BBD7E82FC24366825EA35BE11BCCE76
SHA-256:	91FA41BD434980B288BB645247AC42E80668C865FDCB314DDEA87478CA04D73C
SHA-512:	BCD01AABADADA81FD4DFBDED4631741F1BB8EEEE30CAD76ECDA05285F6E605D569931E17589299AC3CF66AC21A01DC807E558596B04F8DE0D57344549D23DB9E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	
Reputation:	low
Preview:	MDMP..... .....'._.....U.....B.....GenuineIntelW.....T.....'._.....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\WERB1E8.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):	8340
Entropy (8bit):	3.7075069242912075
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLoo6z6YSbSU68ngmfHMISDCprT89b86sfFUm:RrlsNij6z6YeSU68ngmfLSH8Zfz
MD5:	5849A53615CAF332AF88F15726371BA0
SHA1:	A328C8DB9A6101DBFA9352FC4BAB22BA44331FA4
SHA-256:	77CB4C428356ED2B92A41FD9F93594BFBFA6181989B58BA52A230E5CFCED6FA8
SHA-512:	A988F241F981CA7237287B1F92CF46DCCD2FAC8226B9AAE891CDBED2B0C27F262B31C574FF9A648A25651C841FA9D215511C81C556D3DB5DF9F6248252FF509
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.>.4.8.5.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.535803206542934
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9xVWSC8Bng8fm8M4Jgkqk5/kkFx+q8rkDk4wuoYNktvkktVd:uITfj6kSNLJg5IRwG4uHSvkSVd
MD5:	96C86DEC4B5F6644D71A3174CAD6F084
SHA1:	63C06C9B1BA9F7BDF34A9D19A14282E10EE29660
SHA-256:	A04691D185384E54DA71523C2E5F24BD4202B26D8F9CDBEFC4605DE39780913B
SHA-512:	5C3D31BF84A05FE2B30B07D81651C48D509A1B708D7E9C361420ABD2DE90942EE067DCB0F2AF0F0A6EA41C311DB9A9E7ADD2A0B10B95F3D7A0ADC50F8029C DD
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="756191" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.364732034538418
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	CUSTOM SHIPING DOCS.exe
File size:	1651712
MD5:	5533ec4c49c29a1225d1b01d38933bd4
SHA1:	f3aa3401d15d44d65177ba02244c189ee1e822fb

General

SHA256:	ed8bdc7dfb03c556a144b552517f725297acac5c046313b9f8a96432d94cdf5c
SHA512:	0e25a152469a943eb9edc37a753dad54ffec54d434f2ba3d6e4d2a1a65469026ad7ad1868646bd02126488b4b37cbc9ec3b307c768d3224d3d5b9fcdc6cab39c
SSDEEP:	12288:+MwYi7KvtGdcPXZig1LgO5adyneWQ8MCUIFiyS0ry90JrgV9V8+7c:+MR/vtGd6XogRgqlneWMzlJry9mrghc
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|..._.....G.2...H.....`.....@.....`.....

File Icon

Icon Hash:	0f4d494919151b03

Static PE Info

General

Entrypoint:	0x540800
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FC88D7C [Thu Dec 3 07:02:20 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
call 00007FE118D91D95h
pop edx
sub edx, 06h
push edx
xchg ebx, ebx
xchg ecx, ecx
and ecx, ecx
nop
xchg ecx, ecx
xchg ebx, ebx
mov ebx, dword ptr fs:[00000030h]
or ecx, ecx
xchg ecx, ecx
xchg ecx, ecx
mov ebx, dword ptr [ebx+0Ch]
xchg ebx, ebx
mov ebx, dword ptr [ebx+0Ch]
mov ebx, dword ptr [ebx]
xchg ecx, ecx
xchg ebx, ebx
xchg ecx, ecx
and edx, FFFFFFFFh

Instruction
mov ebx, dword ptr [ebx]
and ecx, FFFFFFFFh
and eax, eax
mov eax, dword ptr [ebx+18h]
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [eax+3Ch]
add eax, dword ptr [ebp-04h]
xchg ebx, ebx
xchg ebx, ebx
mov eax, dword ptr [eax+78h]
xchg edx, edx
add eax, dword ptr [ebp-04h]
and ecx, FFFFFFFFh
and ecx, FFFFFFFFh
mov ebx, dword ptr [eax+20h]
nop
add ebx, dword ptr [ebp-04h]
mov ecx, dword ptr [eax+1Ch]
add ecx, dword ptr [ebp-04h]
xchg ebx, ebx
and eax, eax
mov edx, dword ptr [eax+24h]
add edx, dword ptr [ebp-04h]
or ecx, ecx
push ecx
and eax, eax
mov esi, dword ptr [ebx]
or ecx, ecx
and eax, eax
and edx, FFFFFFFFh
add esi, dword ptr [ebp-04h]
and edx, FFFFFFFFh
and ebx, FFFFFFFFh
push edx
push esi
and edx, FFFFFFFFh
xchg edx, edx
call 00007FE118D91E5Ch
or ebx, ebx
or eax, eax
or eax, eax
pop edx
and edx, edx
cmp eax, 0038D13Ch
je 00007FE118D91DA3h
add ebx, 04h
add edx, 02h
jmp 00007FE118D91D56h
or eax, eax
pop ecx
and edx, edx
and ecx, ecx
xor ebx, ebx
xchg ebx, ebx
mov bx, word ptr [edx]
or edx, edx
or ecx, ecx
imul ebx, ebx, 04h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18e000	0x7e62	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13f9ae	0x13fa00	False	0.238771631795	PE32 executable (GUI) Intel 80386, for MS Windows	4.31097129452	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x141000	0x7b8	0x800	False	0.623046875	data	5.6759037632	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x142000	0x4aacf	0x4ac00	False	0.969752691263	data	7.97592063341	IMAGE_SCN_MEM_READ
.tls	0x18d000	0x7c	0x200	False	0.052734375	data	0.118369631259	IMAGE_SCN_MEM_READ
.rsrc	0x18e000	0x7e62	0x8000	False	0.276885986328	data	5.1412464449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x18e144	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x18e5ac	0x10a8	data		
RT_ICON	0x18f654	0x25a8	data		
RT_ICON	0x191bfc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x195e24	0x3e	data		

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:00:35.287821054 CET	65110	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:00:35.398901939 CET	53	65110	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: CUSTOM SHIPING DOCS.exe PID: 4856 Parent PID: 5612

General

Start time:	10:00:32
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\CUSTOM SHIPING DOCS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CUSTOM SHIPING DOCS.exe'
Imagebase:	0x400000
File size:	1651712 bytes
MD5 hash:	5533EC4C49C29A1225D1B01D38933BD4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 6088 Parent PID: 4856

General

Start time:	10:00:33
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4856 -s 216
Imagebase:	0x10a0000
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	6E3D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOMSHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOMSHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	success or wait	1	6E3C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	success or wait	1	6E3C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp.xml	success or wait	1	6E3C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F5C.tmp.csv	success or wait	1	6E3C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F8C.tmp.txt	success or wait	1	6E3C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 c2 27 c9 5f a4 05 12 00 00 00 00 00	MDMP..... .....'_.....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 e0 0b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f8 12 00 00 bf 27 c9 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 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... ....'._.................. ....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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 08 54 00 00 08 54 00 00 20 2a 00 00 08 54 00 00 08 54 00 83 da a6 e8 94 ff 0d 00 00 08 54 00 23 00 00 00 46 02 01 00 84 ff 0d 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.....T...T.. *...T...T..... ......T.#...F.......+.........	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	168	80 16 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 08 54 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 83 da a6 e8 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 8e 0c 00 00	..........................T...	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	20	06 00 00 00 00 20 2a 00 00 00 00 00 98 04 00 00 8a 12 00 00	..... *............	success or wait	6	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	1176	00 00 00 00 ff ff ff ff 00 00 40 00 a0 7b f0 77 38 17 67 00 00 00 00 00 00 00 00 67 00 a0 79 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 f8 7b f0 77 01 00 01 00 00 00 00 00 00 00 eb 7f 00 00 00 00 30 07 eb 7f 00 00 fb 7f 28 02 fc 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 f0 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........@..{.w8.g.......g..y .w................................ {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	5	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	256	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.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 08 54 00 00 08 54 00 00 00 00 00 18 f1 0d 00 bc 9a e5 77 23 00 00 00 06 02 00 00 88 ef 0d 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?........................... ....+...S...+. ..+................T...T..... ....w#...........+.........	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	48	80 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 50 2a 00 00 00 00 00 84 ef 0d 00 00 00 00 00 7c 10 00 00 22 27 00 00 cc 02 00 00 5a 0f 00 00	....P*.......... ..|..."'......Z...	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	52	2e 00 00 00 43 00 55 00 53 00 54 00 4f 00 4d 00 20 00 53 00 48 00 49 00 50 00 49 00 4e 00 47 00 20 00 44 00 4f 00 43 00 53 00 2e 00 65 00 78 00 65 00 00 00	....C.U.S.T.O.M. .S.H.I.P.I.N.G. .D.O.C.S...e.x.e...	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	752	00 00 b6 73 00 00 00 00 00 d0 09 00 8e f6 09 00 51 9e 0f b6 72 0c 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 00 b0 68 02 00 00 00 00 00 30 a2 02 00 00 00 00 b8 1f 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 89 47 03 00 00 00 00 00 b4 4b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4d 9b 1b 00 00 00 00 00 f3 63 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 56 dc 04 00 00 00 00	...s.....Q...r..... .....B.....B?..... .....$..... ..@A.....Zb..... ....h.....0..... .....G.....K .....M.....c..... @.....V.....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	3592	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 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	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0BF.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 64 00 00 00 26 12 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 d0 08 00 00 da 3e 00 00 15 00 00 00 ec 01 00 00 5c 09 00 00 16 00 00 00 98 00 00 00 48 0b 00 00	....4..... ...<.....d. ..&.....T.....8..... ....T.....>..... ..\.....H...	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.8.5.6.<./.P.i.d.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	92	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 43 00 55 00 53 00 54 00 4f 00 4d 00 20 00 53 00 48 00 49 00 50 00 49 00 4e 00 47 00 20 00 44 00 4f 00 43 00 53 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.C.U.S.T.O.M. .S.H.I.P.I.N.G. .D.O.C.S...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 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. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.4.0.2. <./.U.p.t.i.m.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 37 00 39 00 37 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.6.7.9.7.6.9.6. <./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 38 00 38 00 35 00 34 00 34 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.3.8.8.5.4.4.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.9.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 34 00 35 00 33 00 34 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.5.3.4.2.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 34 00 35 00 33 00 34 00 32 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.5.3.4.2.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 33 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.3.1.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.4.0.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.1.6.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.5.1.3.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.5.9.5.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.8.5.1.3.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 32 00 37 00 39 00 38 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.8.2.7.9.8.8.<./.U.p.t.i.m.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 34 00 36 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.4.6.4.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 33 00 37 00 31 00 34 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.3.7.1.4.8.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 33 00 33 00 37 00 38 00 39 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.>.1.0.3.3.7.8.9.4.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 31 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.1.0.7.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 33 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.3.8.4.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 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 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.9.6.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.0.4.4.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 33 00 36 00 38 00 31 00 34 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.3.6.8.1.4.0.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 34 00 39 00 31 00 38 00 34 00 30 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.>.3.4.9.1.8.4.0.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 33 00 36 00 38 00 31 00 34 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.3.6.8.1.4.0.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 30 00 3e 00 43 00 55 00 53 00 54 00 4f 00 4d 00 20 00 53 00 48 00 49 00 50 00 49 00 4e 00 47 00 20 00 44 00 4f 00 43 00 53 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.C.U.S.T.O.M. .S.H.I.P.I.N.G. .D.O.C.S...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 65 00 6b 00 6a 00 70 00 74 00 76 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.>.e.k.j.p.t.v.,. .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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 65 00 6b 00 6a 00 70 00 74 00 76 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.>.e.k.j.p.t.v.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 35 00 37 00 39 00 34 00 30 00 31 00 35 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.>.1.5.5.5.7.9.4.0.1.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 33 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 33 00 34 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.2.-.0.3.T.1.8.:.0.0.:.3.4.Z.".>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 38 00 35 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.2.". .P.I.D.=.".4.8.5.6.". .U.p.t.i.m.e.M.S.=.".5.1.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".5.1.5.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 66 00 34 00 35 00 33 00 64 00 36 00 38 00 2d 00 35 00 61 00 32 00 34 00 2d 00 34 00 65 00 34 00 64 00 2d 00 39 00 65 00 66 00 33 00 2d 00 64 00 37 00 35 00 38 00 34 00 36 00 66 00 38 00 62 00 63 00 35 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.f.4.5.3.d.6.8.-.5.a.2.4.-.4.e.4.d.-.9.e.f.3.-.d.7.5.8.4.6.f.8.b.c.5.e.<./.G.u.i.d.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 33 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 33 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.2.-.0.3.T.1.8.:.0.0.:.3.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.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	6E3C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB286.tmp.xml	unknown	4630	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	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOM SHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a\Report.wer	unknown	2	ff fe	..	success or wait	1	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOM SHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a\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	135	6E3C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_CUSTOM SHIPING D_ab7019a57941d055ca75d96ef7ee3b39da4f9ae0_41b924a0_1781b95a\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 35 00 31 00 39 00 39 00 35 00 32 00 31 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.3.5.1.9.9.5.2.1.4.	success or wait	1	6E3C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	success or wait	1	6E3E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E3E1FB2	RegCreateKeyExW
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	ProgramId	unicode	0006c4324ae7c4776a8e796c38da63f404c50000ffff	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	FileId	unicode	0000f3aa3401d15d44d65177ba02244c189ee1e822fb	success or wait	1	6E3E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	LowerCaseLongPath	unicode	c:\users\user\desktop\custom shiping docs.exe	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	LongPathHash	unicode	custom shiping d|a2c6c1f9	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	Name	unicode	custom shiping docs.exe	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	Publisher	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	Version	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	BinFileVersion	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	BinaryType	unicode	pe32_i386	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	ProductName	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	ProductVersion	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	LinkDate	unicode	12/03/2020 07:02:20	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	BinProductVersion	unicode		success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	Size	B	00 34 19 00 00 00 00 00	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	Language	dword	0	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	IsPeFile	dword	1	success or wait	1	6E3E36BF	unknown
\REGISTRY\A\{da6765f6-3bcf-4bce-24b7-c9f9d4be8498}\Root\InventoryApplicationFile\custom shiping d|a2c6c1f9	IsOsComponent	dword	0	success or wait	1	6E3E36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 08 54 00 02 00 00 00 01 00 00 00 83 DA A6 E8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E3E1FE8	RegSetValueExW

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

Disassembly

Code Analysis