

JoeSandbox Cloud BASIC



ID: 346431

Sample Name: jesovROZ8A.exe

Cookbook: default.jbs

Time: 15:51:17

Date: 31/01/2021

Version: 31.0.0 Emerald

Table of Contents

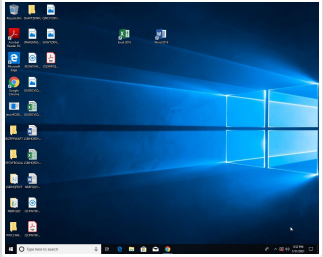
Table of Contents	2
Analysis Report jesovROZ8A.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
AV Detection:	5
Compliance:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	10
General	10
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	13
Sections	13
Resources	13
Imports	14
Version Infos	14
Possible Origin	14
Network Behavior	14
UDP Packets	14
Code Manipulations	15
Statistics	15
Behavior	15
System Behavior	15
Analysis Process: jesovROZ8A.exe PID: 2416 Parent PID: 5632	15

General	15
Analysis Process: WerFault.exe PID: 5888 Parent PID: 2416	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Written	17
Registry Activities	39
Key Created	39
Key Value Created	39
Disassembly	40
Code Analysis	40

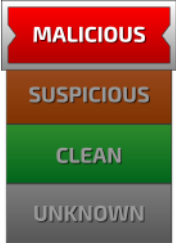
Analysis Report jesovROZ8A.exe

Overview

General Information

Sample Name:	jesovROZ8A.exe
Analysis ID:	346431
MD5:	039ce25d495fa55..
SHA1:	6684d0fde17405..
SHA256:	94fff127753ed1d...
Tags:	unnamed3
Most interesting Screenshot:	
	

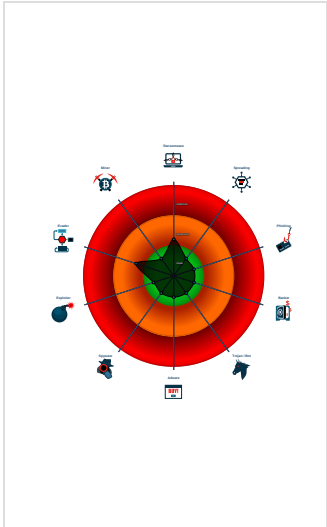
Detection

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

Signatures

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

Classification



Startup

■ System is w10x64
●  jesovROZ8A.exe (PID: 2416 cmdline: 'C:\Users\user\Desktop\jesovROZ8A.exe' MD5: 039CE25D495FA555AE1C210592B564D0)
●  WerFault.exe (PID: 5888 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2416 -s 588 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
■ cleanup

Malware Configuration

No configs have been found

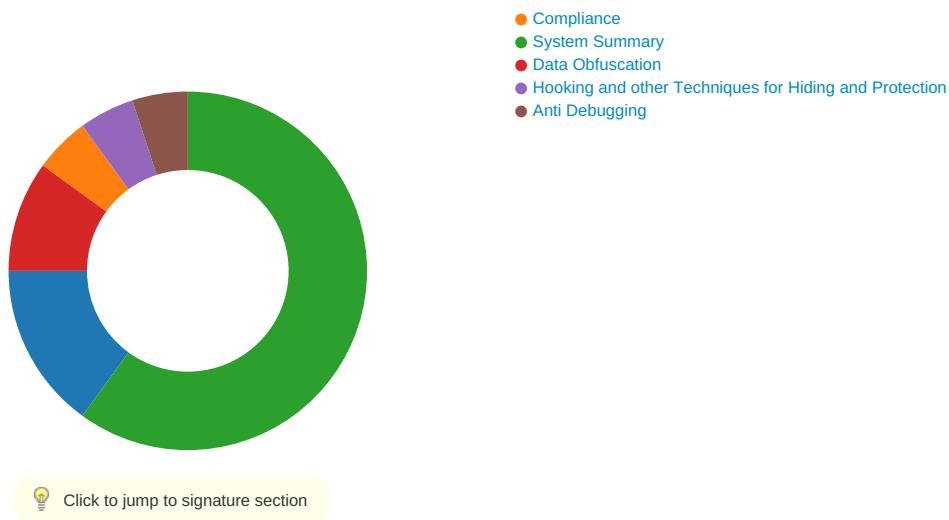
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

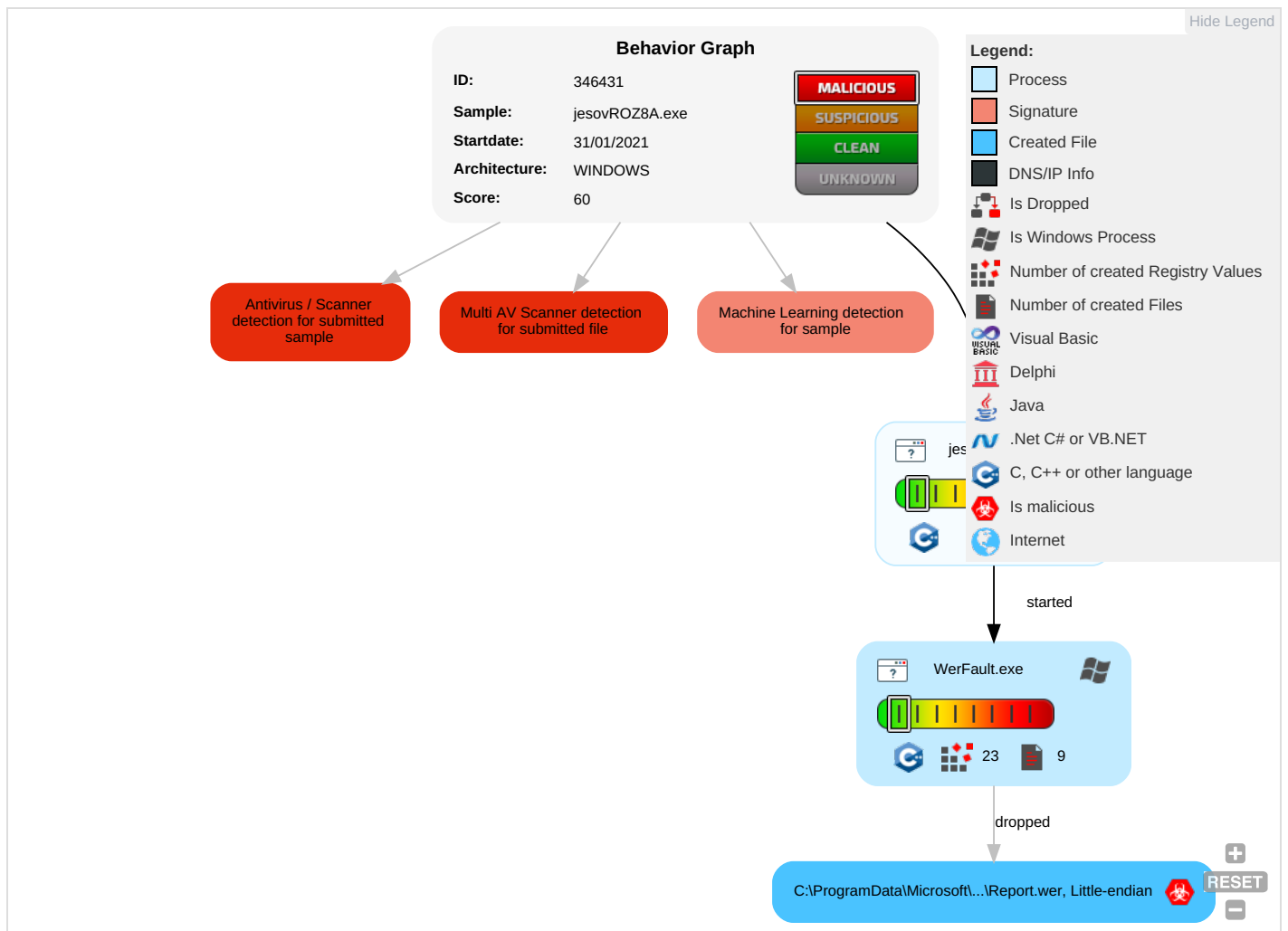


Uses 32bit PE files

Mitre Att&ck Matrix

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

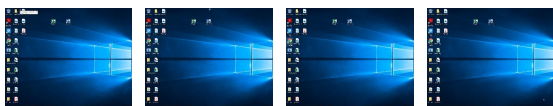
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346431
Start date:	31.01.2021
Start time:	15:51:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jesovROZ8A.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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winEXE@2/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.3% (good quality ratio 69.3%) • Quality average: 46.9% • Quality standard deviation: 34.2%
HCA Information:	Failed
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 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.255.188.83, 104.43.193.48 • Excluded domains from analysis (whitelisted): skypedataprdrdcowus17.cloudapp.net, skypedataprdrdcowus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, skypedataprdrdcowus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609f
elReport.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11734
Entropy (8bit):	3.7756645450844095
Encrypted:	false
SSDEEP:	192:d6lo4/KjHBUZMXYjRWV//u7s7S274ltDX2:H4/+BUZMXYjM/u7s7X4ltDX2
MD5:	90348400B8FF91427A3D8FE633406DAD
SHA1:	B0890BF3F5D23484AE45B77C2B2916D01DB734BF
SHA-256:	B896514327C8A7E71B11B5A09D4C29C3A0300D34BA416416CF6E4FA8483053C2
SHA-512:	B8A9BB49180A44760BE185E39C8BBC696E60DCAF8ED4723B80E7A00034E1DDB5F0AA69D972B22B0EABC5E0958AD76029F32DEE513842759525EBA0B618A304C9
Malicious:	true
Reputation:	low
Preview:	..Version.=1.....Event.Type.=A.P.P.C.R.A.S.H.....Event.Time.=1.3.2.5.6.6.1.0.7.2.4.8.0.7.9.4.8.5.....Report.Type.=2.....Consent.=1.....Up.Lo.ad.Ti.me.=1.3.2.5.6.6.1.0.7.2.5.5.7.9.5.0.1.....Report.Status.=2.6.8.4.3.5.4.5.6.....Report.Identifier.=7.1.6.b.8.a.4.8.-.6.5.c.0.-.4.2.2.5.-.a.6.c.8.-.2.3.9.f.a.8.7.2.9.c.c.e.....I.n.t.e.g.r.a.t.o.r.Re.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=d.6.7.8.e.b.2.4.-.7.c.1.1.-.4.3.c.8.-.a.2.a.e.-.5.a.9.c.0.8.1.4.d.4.9.7.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.ue.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=j.e.s.o.v.R.O.Z.8.A...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=C.h.e.v.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.9.7.0.-0.0.0.1.-0.0.1.7.-.1.5.d.5.-.a.2.1.2.2.c.f.8.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.6.3.e.9.9.7.4.9.2.3.7.a.0.6.0.7.c.4.b.f.6.b.d.7.1.4.a.8.4.d.c.b.3.0.0.0.0.9.0.4.!0.0.0.0.6.6.8.4.d.0.f.f.d.e.1.7.4.0.5.2.a.0.3.9.3.1.9.8.1.2.6.2.d.c.0.a.7.c.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	
Category:	dropped
Size (bytes):	8282
Entropy (8bit):	3.6994579938462806
Encrypted:	false
SSDEEP:	192:RrI7r3GLNijt6jfy6YS/SUIUpblGgmfPjStCprF89brnesfH5m:RrlsNip6e6YqSUIU+gmfPjS/rndfU
MD5:	3BAD7B2DBEFB569A73D48F4E1BDBE508
SHA1:	8573B937AC58F6F45B2ABFDE4444E5EE9D0B382B
SHA-256:	794287A06E613B335CCBDB4141CAF7A8D2B5E3EC8B67905360FEA6DE030DBBB5
SHA-512:	30A5B628C11FD517627724BB6B40E3A587E33047F685365AA264D4AF2580A626B3D94D6DD8E5E55F9B498624AF3B615139558106B26079926CDF91F8FBED36FC
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.>2.4.1.6.<./P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.459246142148875
Encrypted:	false
SSDEEP:	48:cvlwSD8zs8tJgtWI98/EWSC8B1/8fm8M4JosSFL+q8qrVZ5P9M0h4sd:ulTf8HNdSNsJ8tZ5P9MCdd
MD5:	EE9A37A7CF7A48B561CE809E0A9FD314
SHA1:	7A53D5C095AE88DB6527D23ED6F1828661065825
SHA-256:	3A7ACD8DFC4FFB86D5B8D14C837E25B5E82FCC2B699CAA7E3B5DA2EF2A1660FF
SHA-512:	27B92BA14C832DCDC77EFA83CDA0CB756907858062DB83C14A435ACE13D716A2EA8F58C7230016101D5410A3265994B3358B1E73AF41405BEE8B062AD6910DE
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="verblid" 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="841502" />.. <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" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Jan 31 23:52:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	41942
Entropy (8bit):	2.338919342839634
Encrypted:	false
SSDEEP:	192:/N/t2P6MvHmWzxUsxtr+AkK2VOD+wGt6t5Q3KrRMjCTx/aE6MC:GuWzxUsxx+bgTsZKruCTpP6MC
MD5:	EF41E4BCD97E9BF8344AE871265D27F2
SHA1:	5013FCE08852EA3B415DC5B9B0F312DD1D1DDE18
SHA-256:	FDD7E4E2E749661B7BBEB808272674283A5FA9D0E13AE47EE71D8B9E0F118D0C
SHA-512:	9ED65096CD14476E73D7BD6503BDB5B496715968DBA737832EA936478A2FF314931D3D9AB97450AF2831D870A93A423CF2CA7C6BD337437F564F5638EAF619A9
Malicious:	false
Reputation:	low
Preview:	MDMP.....B.`.....U.....B.....GenuineIntelW.....T.....p...B.`.....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.....

Static File Info

General

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.917886227244785
TrID:	- Win32 Executable (generic) a (10002005/4) 99.39% - UPX compressed Win32 Executable (30571/9) 0.30% - Win32 EXE Yoda's Crypter (26571/9) 0.26% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02%
File name:	jesovROZ8A.exe
File size:	202240
MD5:	039ce25d495fa555ae1c210592b564d0
SHA1:	6684d0ffde174052a03931981262dc0a7cb9891c
SHA256:	94fff127753ed1d704c781b5c391f5e62f4a907b67f7e1d51c3c84add5851ab
SHA512:	c2be8d6b80e57339957f370b4ac31bd03140f9a9ed4865926eb6d7e5a69d3510b046930c1933d38629b4c3bcae007b6cf5e6140463ab6e064820cdd91bbd46bb
SSDEEP:	3072:RD9PfpJ/v2bIfdjba+htCsw0qv2AYjGX9E7e+q8EOADhpsWgXDeet78Bx/rUyMHL:RXJWbUTwsTqvdMO9nnSmphgTeE4B+8U
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......F...!.. '.....h%.....'...k...'.0...C'...y...&...<&...%.....&...^....%...w.. .&...3...\$.....\$....7..Z&..Rich.'

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x445590
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4D771DAA [Wed Mar 9 06:26:50 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	8
OS Version Minor:	2
File Version Major:	8
File Version Minor:	2
Subsystem Version Major:	8
Subsystem Version Minor:	2
Import Hash:	976c9384d1a3c367e491662f20af4316

Entrypoint Preview	
Instruction	
pushad	
mov esi, 00416000h	
lea edi, dword ptr [esi-00015000h]	
push edi	
jmp 00007F753091967Dh	
nop	
mov al, byte ptr [esi]	
inc esi	
mov byte ptr [edi], al	
inc edi	

Instruction
add ebx, ebx
jne 00007F7530919679h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F753091965Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F7530919679h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F7530919661h
jne 00007F753091967Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F7530919656h
xor ecx, ecx
sub eax, 03h
jc 00007F753091967Fh
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F75309196E6h
mov ebp, eax
add ebx, ebx
jne 00007F7530919679h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jne 00007F7530919679h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jne 00007F7530919692h
inc ecx
add ebx, ebx
jne 00007F7530919679h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F7530919661h
jne 00007F753091967Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F7530919656h
add ecx, 02h
cmp ebp, FFFFF300h
adc ecx, 01h
lea edx, dword ptr [edi+ebp]
cmp ebp, FFFFFFFCh
jbe 00007F7530919681h
mov al, byte ptr [edx]
inc edx

Instruction

mov byte ptr [edi], al

inc edi

dec ecx

jne 00007F7530919669h

jmp 00007F75309195D8h

nop

mov eax, dword ptr [edx]

add edx, 04h

mov dword ptr [edi], eax

add edi, 04h

sub ecx, 04h

jnb 00007F7530919663h

add edi, ecx

jmp 00007F75309295C1h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4749c	0x428	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x46000	0x149c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x15000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x16000	0x30000	0x2f800	False	0.996900699013	data	7.94664222533	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x2000	0x1a00	False	0.621394230769	data	5.74902503533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

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

Name	RVA	Size	Type	Language	Country
None	0x4747c	0x5	data	English	United States
None	0x47488	0x5	data	English	United States
None	0x47494	0x5	data	English	United States

Imports

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

Version Infos

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

Possible Origin

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

Network Behavior

UDP Packets

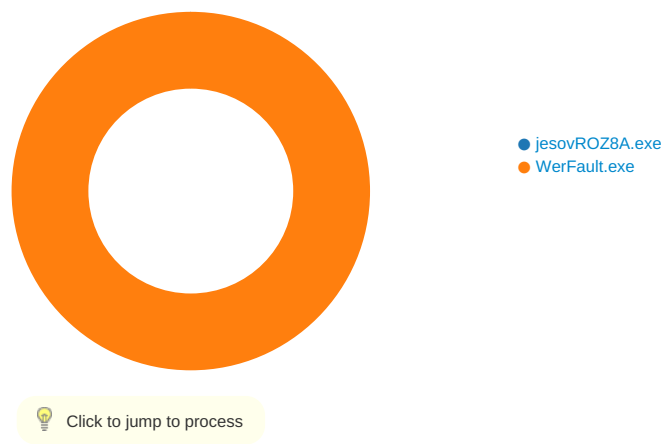
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2021 15:51:57.030225039 CET	53	55984	8.8.8.8	192.168.2.3
Jan 31, 2021 15:51:58.114346027 CET	64185	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:51:58.171156883 CET	53	64185	8.8.8.8	192.168.2.3
Jan 31, 2021 15:51:59.309480906 CET	65110	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:51:59.357852936 CET	53	65110	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:00.330826044 CET	58361	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:00.380363941 CET	53	58361	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:01.876180887 CET	63492	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:01.927094936 CET	53	63492	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:02.834682941 CET	60831	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2021 15:52:02.882750988 CET	53	60831	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:03.956110001 CET	60100	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:04.009675980 CET	53	60100	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:05.175945997 CET	53195	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:05.223980904 CET	53	53195	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:05.743197918 CET	50141	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:05.802350044 CET	53	50141	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:06.373653889 CET	53023	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:06.421638012 CET	53	53023	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:07.194112062 CET	49563	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:07.242078066 CET	53	49563	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:08.044931889 CET	51352	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:08.095187902 CET	53	51352	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:09.233760118 CET	59349	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:09.292754889 CET	53	59349	8.8.8.8	192.168.2.3
Jan 31, 2021 15:52:10.289381981 CET	57084	53	192.168.2.3	8.8.8.8
Jan 31, 2021 15:52:10.337560892 CET	53	57084	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: jesovROZ8A.exe PID: 2416 Parent PID: 5632

General	
Start time:	15:52:02
Start date:	31/01/2021
Path:	C:\Users\user\Desktop\jesovROZ8A.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\jesovROZ8A.exe'
Imagebase:	0x400000
File size:	202240 bytes

MD5 hash:	039CE25D495FA555AE1C210592B564D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 5888 Parent PID: 2416

General

Start time:	15:52:03
Start date:	31/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2416 -s 588
Imagebase:	0x230000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6E041717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609fe	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609fe\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6E03497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp	success or wait	1	6E03497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp.xml	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER705A.tmp.csv	success or wait	1	6E034BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER706B.tmp.txt	success or wait	1	6E034BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a5 42 17 60 a4 05 12 00 00 00 00 00	MDMP.....B.`.....	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.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 dc 1b 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 70 09 00 00 a2 42 17 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 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... ...p...B.`.....0..2..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 bc 11 00 00 9c 07 00 00 05 00 00 00 24 01 00 00 e2 2b 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 80 17 00 00 9e 8c 00 00 15 00 00 00 ec 01 00 00 58 19 00 00 16 00 00 00 98 00 00 00 44 1b 00 00	\$. ...+.....T.....8..... ...T..... ..X.....D..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?.x.m.l..v.e.r.s.i.o.n.=." 1...0". .e.n.c.o.d.i.n.g.=." U.T.F.-.1.6."?>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a d.a.t.a.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s. i.o.n.>.1.0...0. </.W.i.n.d.o.w. s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.</.B. u.i.l.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t>.(.0.x.3.0.). :. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./P.r.o.d.u.c.t>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n>.P.r.o.f.e.s.s.i.o.n.a.l.<./E.d.i.t.i.o.n>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.<./B.u.i.l.d.S.t.r.i.n.g>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n>.1.<./R.e.v.i.s.i.o.n>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./F.l.a.v.o.r>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./L.C.I.D.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 34 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.4.1.6.<./P.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6a 00 65 00 73 00 6f 00 76 00 52 00 4f 00 5a 00 38 00 41 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.j.e.s.o.v.R.O.Z.8.A...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 31 00 36 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.>.2.4.1.6.<./U.p.t.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4.g.u.e.s.t.= ".3.3.2".h.o.s.t.= ".3.4.4.0.4.">.>.1.<./W.o.w.6.4.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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	<.l.p.t.E.n.a.b.l.e.d.>.0.<./l.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 36 00 36 00 34 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.1.6.6.4.3.8.4.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 36 00 34 00 30 00 33 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.0.6.4.0.3.8.4.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 39 00 39 00 34 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.>.1.9.9.4.</.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 38 00 34 00 30 00 39 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.>.7.6.8.4.0.9.6.</.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 38 00 34 00 30 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.6.8.4.0.9.6.</.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.4.9.6.0.</.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.1.7.3.7.8.4.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.3.7.4.4.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.3.4.7.2.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.2.0.2.7.5.2.0.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 33 00 35 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.0.3.5.7.1.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 32 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.0.2.7.5.2.0.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./P.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.8.0.0.0.4.0.0.5.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 38 00 36 00 35 00 33 00 35 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.>.4.5.8.6.5.3.5.<./U.p.t.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<W.o.w.6.4.g.u.e.s.t.="0".h.o.s.t.="3.4.4.0.4.">.0.<./W.o.w.6.4.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 35 00 37 00 37 00 34 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.>.4.5.7.7.4.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 38 00 36 00 36 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.3.8.6.6.3.6.8.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 35 00 33 00 30 00 34 00 39 00 36 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.>.1.0.3.5.3.0.4.9.6.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 34 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.9.6.4.6.4.8.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 32 00 38 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.9.2.8.9.6.8.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 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 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>.7.2.9.1.2.<./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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.7.0.7.2.0.<./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	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 32 00 31 00 35 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>. 3.5.2.2.1.5.0.4. <./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 32 00 31 00 36 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.2.1.6.2.5.6. <./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 32 00 31 00 35 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.2.2.1.5.0.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H. <./E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6a 00 65 00 73 00 6f 00 76 00 52 00 4f 00 5a 00 38 00 41 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<P.a.r.a.m.e.t.e.r.0.>.j.e.s.o.v.R.O.Z.8.A...e.x.e. <./P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./M.I.D.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 6c 00 64 00 6c 00 6c 00 76 00 77 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.>.I.d.I.l.v.w.,.I.n.c...<./S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 6c 00 64 00 6c 00 6c 00 76 00 77 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>.I.d.I.l.v.w.7.,.1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.</.B.I.O.S.V.e.r.s.i.o.n>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 34 00 32 00 32 00 36 00 33 00 37 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e>.1.5.6.4.2.2.6.3.7.0.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.</.O.S.I.n.s.t.a.l.l.T.i.m.e>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>. 0.8.:0.0. <./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0. <./U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0. <./F.l.a.g.s.>.	success or wait	3	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./I.n.t.e.g.r.a.t.o.r.>	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 33 00 31 00 54 00 32 00 33 00 3a 00 35 00 32 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-.0.1.-.3.1.T.2.3.:.5.2:.. 0.5.Z.">.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 34 00 31 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 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.l.d.= ".3.3.7". .P.I.D.= ".2.4.1.6". .U.p.t.i.m.e.M.S.= ".3.5.9". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".3.5.9". .S.u.s.p.e.n.d.e.d.M.S.= ".0". .H.a.n.g.C.o.u.n.t.= ".0". .G.h.o.s.t.C.o.u.n.t.= ".0". .C.r.a.s.h.e.d.= ".1."	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.r.o.c.e.s.s.>	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 31 00 36 00 62 00 38 00 61 00 34 00 38 00 2d 00 36 00 35 00 63 00 30 00 2d 00 34 00 32 00 32 00 35 00 2d 00 61 00 36 00 63 00 38 00 2d 00 32 00 33 00 39 00 66 00 61 00 38 00 37 00 32 00 39 00 63 00 63 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.7.1.6.b.8.a.4.8-.6.5.c.0.-4.2.2.5.-a.6.c.8-.2.3.9.f.a.8.7.2.9.c.c.e.<./G.u.i.d.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 33 00 31 00 54 00 32 00 33 00 3a 00 35 00 32 00 3a 00 30 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-0.1.-3.1.T.2.3.:5.2.:0.5.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32A.tmp.xml	unknown	4622	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.. ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609fe\Report.wer	unknown	2	ff fe	..	success or wait	1	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609fe\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	173	6E03497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_jesovROZ8A.exe_43fc5ffcbae1f11637667ee26b773884583759_76289d07_174609fe\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 2d 00 37 00 34 00 39 00 34 00 32 00 38 00 36 00 35 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .7.4.9.4.2.8.6.5.7.	success or wait	1	6E03497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0536BF	unknown
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0536BF	unknown
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\jesovroz8a.exe 70a5129d	success or wait	1	6E0536BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E051FB2	RegCreateKeyExW
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0343D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\jesovroz8a.exe 70a5129d	ProgramId	unicode	00063e99749237a0607c4bf6bd714a84dcb300000904	success or wait	1	6E0536BF	unknown
\REGISTRYA\{25e27cb3-da46-cb38-f2a2-6c625415d566}\Root\InventoryApplicationFile\jesovroz8a.exe 70a5129d	FileId	unicode	00006684d0ffde174052a03931981262dc0a7cb9891c	success or wait	1	6E0536BF	unknown

