ID: 323458
Sample Name: INV.exe
Cookbook: default.jbs
Time: 02:12:40
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

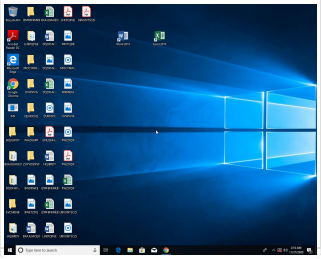
Analysis Report INV.exe

Overview

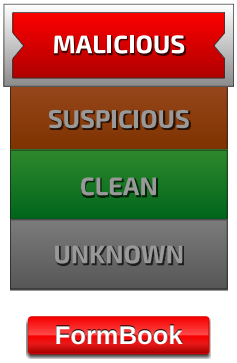
General Information

Sample Name:	INV.exe
Analysis ID:	323458
MD5:	83259cb8264266..
SHA1:	180e81bab341ed..
SHA256:	6e28207e7a3ef7f..
Tags:	exe

Most interesting Screenshot:



Detection

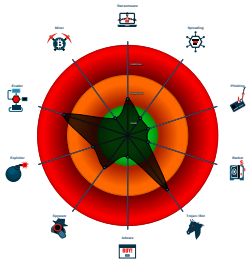


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- INV.exe (PID: 6580 cmdline: 'C:\Users\user\Desktop\INV.exe' MD5: 83259CB8264266650327823342 1C306D)
  - conhost.exe (PID: 6592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - INV.exe (PID: 6640 cmdline: C:\Users\user\Desktop\INV.exe MD5: 83259CB8264266650327823342 1C306D)
    - WerFault.exe (PID: 6752 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 872 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1ac18:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ae92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x269b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x264a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x26ab7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x26c2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1b8aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2571c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1c5a3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2c827:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2d82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x29749:$sqlite3step: 68 34 1C 7B E1 • 0x2985c:$sqlite3step: 68 34 1C 7B E1 • 0x29778:$sqlite3text: 68 38 2A 90 C5 • 0x2989d:$sqlite3text: 68 38 2A 90 C5 • 0x2978b:$sqlite3blob: 68 53 D8 7F 8C • 0x298b3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000003.645815699.0000000000D26000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000003.645815699.0000000000D26000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9050:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x92ca:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14ded:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x148d9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14eef:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15067:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x9ce2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x13b54:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa9db:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ac5f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc62:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

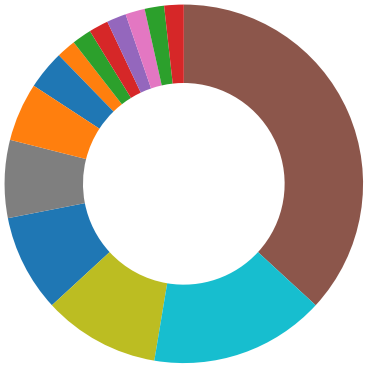
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.INV.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.INV.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1e940:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ebba:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2a6dd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2a1c9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2a7df:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2a957:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1f5d2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x29444:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x202cb:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x3054f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x31552:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.INV.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x2d471:$sqlite3step: 68 34 1C 7B E1 • 0x2d584:$sqlite3step: 68 34 1C 7B E1 • 0x2d4a0:$sqlite3text: 68 38 2A 90 C5 • 0x2d5c5:$sqlite3text: 68 38 2A 90 C5 • 0x2d4b3:$sqlite3blob: 68 53 D8 7F 8C • 0x2d5db:$sqlite3blob: 68 53 D8 7F 8C
2.2.INV.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.INV.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1ad40:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1afba:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x26add:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x265c9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x26bdf:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x26d57:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1b9d2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x25844:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1c6cb:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2c94f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2d952:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

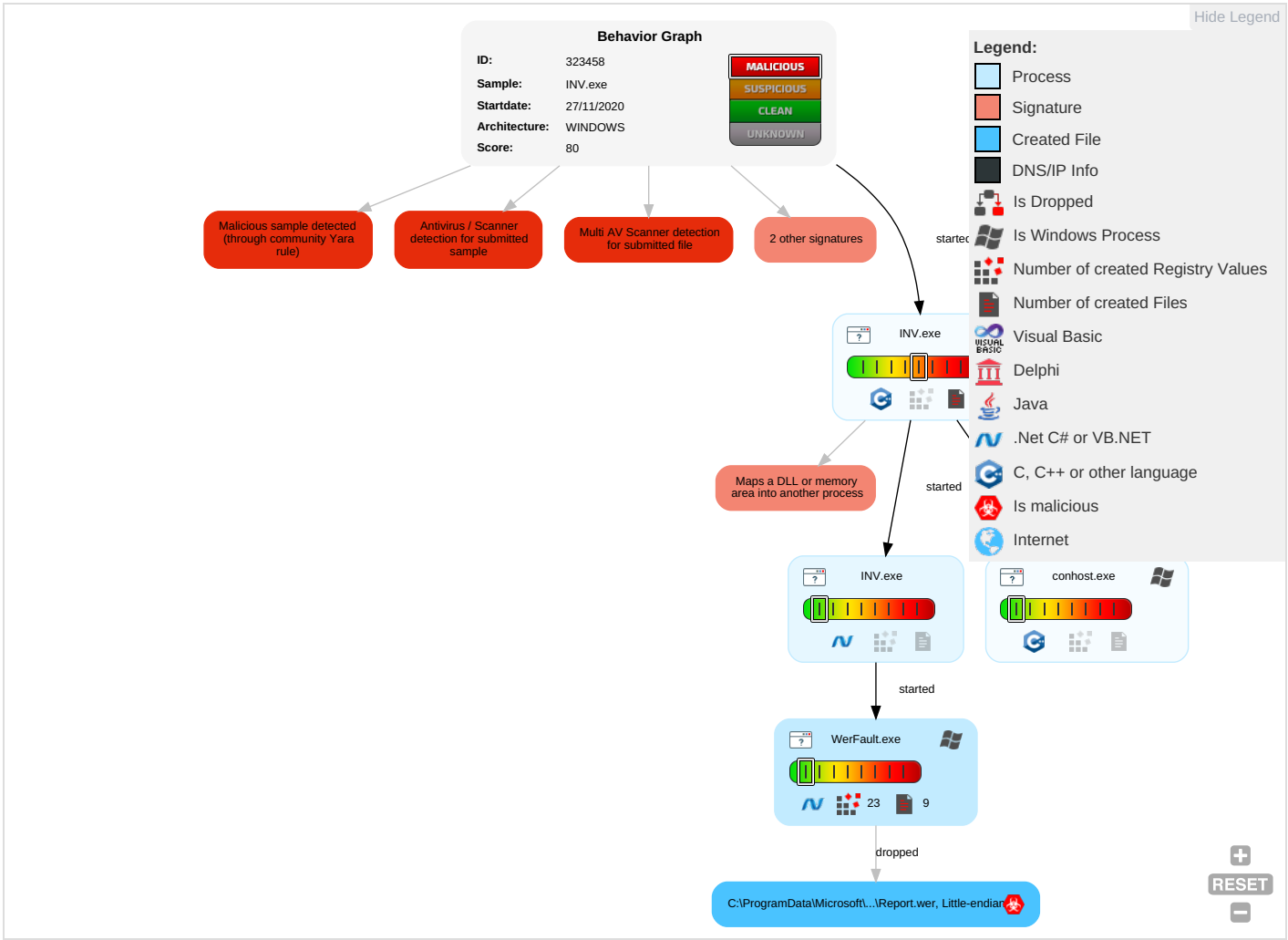
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 1	Modify Registry 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Networ Commu
Default Accounts	Scheduled Task/Job	Application Shimming 1	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit Redirec Calls/SI

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Disable or Modify Tools 1	Security Account Manager	Security Software Discovery 6 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit S Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue \ Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 3 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco

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
INV.exe	37%	Virustotal		Browse
INV.exe	100%	Avira	ADWARE/MultiPlug.Gen7	
INV.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.INV.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.INV.exe.90000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
2.0.INV.exe.90000.0.unpack	100%	Avira	ADWARE/MultiPlug.Gen7		Download File
0.0.INV.exe.90000.0.unpack	100%	Avira	ADWARE/MultiPlug.Gen7		Download File
2.2.INV.exe.90000.0.unpack	100%	Avira	ADWARE/MultiPlug.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000005.00000003.653666644.0000000004CE0000.00000004.00000001.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323458
Start date:	27.11.2020
Start time:	02:12:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV.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:	28
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:	mal80.troj.evad.winEXE@5/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51% (good quality ratio 47.8%) • Quality average: 80.9% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, wermgr.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 13.88.21.125, 51.104.139.180, 51.11.168.160, 92.122.213.247, 92.122.213.194, 40.90.23.206, 40.90.23.247, 40.90.23.208, 40.90.137.126, 13.104.215.69, 40.90.137.124, 40.90.23.154, 40.90.137.125, 20.54.26.129, 92.122.145.220, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, blu-main-ips-v4only.b.lg.prod.aadmsa.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11314
Entropy (8bit):	3.7650886089164053
Encrypted:	false
SSDEEP:	96:O8CEsLPcDl+hVkDNfypXIQcQvc6QcEDMcw3Db+HbHgg5uHjgtYsaSiYuka5o1CvY:EEIUZMHBUZMXYjGd/u7sJS274It56b
MD5:	4210E4EFCE813821ABC85A05EC9BB610
SHA1:	9C7923F645EEA0C831209F1C7CC561D9A4E98A37
SHA-256:	5282B268BBFA8CDB2BBA05CBDFAD1461B0B3BCEFF4CEC6B9BE76937439E00078
SHA-512:	2B1BC2DACE8AE82B733B5802BA299E6AB5C3E2665E2B43B97CC9F4F444429AC23C26BCA035AC2DE02EB6FCE4397566F906C0A30E53DC0755DBFD969D4D52142
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.9.1.3.2.0.9.6.8.5.3.1.1.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.9.1.3.2.1.3.5.4.4.6.7.6.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.6.c.f.0.5.4.5.-.1.6.d.1.-.4.f.e.4.-.9.a.7.8.-.3.2.5.8.c.3.e.4.0.c.d.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.a.7.3.4.8.b.e.-.5.9.3.e.-.4.1.c.9.-.b.b.0.5.-.b.d.c.8.0.a.6.e.2.7.c.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.N.V...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.f.0.-.0.0.0.1.-.0.0.1.b.-.8.c.a.5.-.8.5.8.1.5.a.c.4.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.9.d.3.5.a.e.9.1.5.c.2.c.9.6.f.c.6.d.3.6.c.e.5.2.8.8.0.2.e.4.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.8.0.e.8.1.b.a.b.3.4.1.e.d.a.0.d.4.0.4.b.8.f.5.f.e.d.9.3.b.c.3.b.3.5.0.c.f.b.d.!.I.N.V...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Nov 27 01:13:30 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	107650
Entropy (8bit):	3.5546107077695166
Encrypted:	false
SSDEEP:	768:mQMS9C5l3JN1OpTwebzkmRf6mx303oHqUD8CQjMOWQaCgUziU5Sep9qaLa+97h:mld9e/x303oGFBNaCgUziUzpsq7h
MD5:	51279CD356C366D625D183A3DCB83674
SHA1:	931A15B368662F913082F6675C1E5E4F328C4924
SHA-256:	0716B41901C75AD657AE2BC6658506EF633A026CE2C0D547AC8A9218E6FC464A
SHA-512:	260521156C984B18DABFF4F9A993596F431BDA436BB50E987B755868BEE1B5113163E9BE06327D22CDAB3260359656F0F60C80999B5DE340A5C1D14F50CA4EA2
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....R._.....U.....B.....GenuineIntelW.....T.....R._.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8222
Entropy (8bit):	3.693586025165365
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8v62X6YZH6tppgmfZ2SN+pr589bWW7wsfGSm:RrlsNiE6A6Yp6tppgmfZ2S/WYfa
MD5:	7FF269553DEC8C3DEAD9D42A93981584
SHA1:	36D14895C4F350E51AA8E7D8ADFB9D9F5B1D6CD1
SHA-256:	FFA7AD16F540827A13964F1FBF690B75D32B6519B24CACE7E73AB264C77691A7
SHA-512:	C6249B20B3821B02487999FF74C631E49547E1548F3498CFF666CE74C08A87BE4EE16150C6ABB3FDFADB738FCEC96C3086D6C10EA10E1C0C096D5BFF1CE5DF6
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp.xml	
Category:	dropped
Size (bytes):	4533
Entropy (8bit):	4.453085391753248
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8JgtWI98SWSC8Bq8fm8M4JA+ZFX+q8Hxq7zqvJuBd:uITf6bzSNlJnDII7mv4Bd
MD5:	621C78EE612AFF1724CCA4B31846DCB9
SHA1:	3FC8DE4A557EF3759869FE51F5D9E36BFD6F2679
SHA-256:	C36F1AFCB9B5FA8B1E9CBA499B001AE3352C7242E6D9E3574B4785A218911D08
SHA-512:	C578049B7162B750EFB0BED6451DF9DB3024917A10ABA87616E7B6EA975F7EBA1FDEFCBA6FF86AC8AD4EDBEDFB213430FD22248076A4FAC866CCFBD5229F2A87
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="746544" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.734539190231703
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	INV.exe
File size:	394240
MD5:	83259cb826426665032782334 21c306d
SHA1:	180e81bab341eda0d404b8f5fed93bc3b350cfbd
SHA256:	6e28207e7a3ef7f173d7a7905208a55ff0ad1eb645241e2e9ae453c643cf3a31
SHA512:	c5b2342cdd849a49b4e2472c563301aa3f69d192317901 13dd94db5ad680db7b6e529a6b23fd2528e6378a08f058 e06a9663c8539ce44655235fd241cdc5c7
SSDEEP:	6144:OKRY0sMhL5VwjYGFzVfPn1IqXJ7kELwepHTAXF3QOrIxc8V4rJH:OKBsM1whBPn1IWdkELLpHU1Xrmc8V4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0Y.ecY.ecY.ec...c@.ec...cV.ec...c<.ec.S.cT.ecY.dc3.ecT..cX.ecT..cX.ecY..cX.ecT..cX.ecRichY.ec.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40127b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

General

Time Stamp:	0x5FC0322D [Thu Nov 26 22:54:37 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e5251995cfb2fe7a12656fff0fe17665

Entrypoint Preview

Instruction
call 00007FAD40BC234Eh
jmp 00007FAD40BC0D8Ah
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
mov eax, dword ptr [eax]
cmp dword ptr [eax], E06D7363h
jne 00007FAD40BC0F77h
cmp dword ptr [eax+10h], 03h
jne 00007FAD40BC0F71h
mov eax, dword ptr [eax+14h]
cmp eax, 19930520h
je 00007FAD40BC0F6Dh
cmp eax, 19930521h
je 00007FAD40BC0F66h
cmp eax, 19930522h
je 00007FAD40BC0F5Fh
cmp eax, 01994000h
je 00007FAD40BC0F58h
xor eax, eax
pop ebp
retn 0004h
call 00007FAD40BC26ECh
int3
push 00401285h
call 00007FAD40BC2D3Bh
pop ecx
xor eax, eax
ret
push ebp
mov ebp, esp
push esi
call 00007FAD40BC128Eh
mov esi, eax
test esi, esi
je 00007FAD40BC109Bh
mov edx, dword ptr [esi+5Ch]
mov ecx, edx
push edi
mov edi, dword ptr [ebp+08h]
cmp dword ptr [ecx], edi
je 00007FAD40BC0F5Fh
add ecx, 0Ch
lea eax, dword ptr [edx+00000090h]
cmp ecx, eax
jc 00007FAD40BC0F41h
lea eax, dword ptr [edx+00000090h]
cmp ecx, eax
jnc 00007FAD40BC0F56h
cmp dword ptr [ecx], edi

Instruction
je 00007FAD40BC0F54h
xor ecx, ecx
test ecx, ecx
je 00007FAD40BC1066h
mov edx, dword ptr [ecx+08h]
test edx, edx
je 00007FAD40BC105Bh
cmp edx, 05h
jne 00007FAD40BC0F5Eh
and dword ptr [ecx+08h], 00000000h
xor eax, eax
inc eax
jmp 00007FAD40BC104Bh
cmp edx, 01h
jne 00007FAD40BC0F5Ah
or eax, FFFFFFFFh
jmp 00007FAD40BC103Eh

Rich Headers

Programming Language:	• [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d124	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x63000	0x130c	.reloc
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	0x1cc68	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x1c0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16e9f	0x17000	False	0.517747961957	data	6.61669655756	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x5bb4	0x5c00	False	0.373259171196	data	4.5684318813	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e000	0x43b44	0x41e00	False	0.988499911053	DOS executable (block device driver\377\377\200)	7.98533790258	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x1e0	0x200	False	0.52734375	data	4.70436301348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x63000	0x130c	0x1400	False	0.778515625	data	6.50096033347	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x62060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	EnumCalendarInfoExA, SetCalendarInfoW, VirtualProtect, CloseHandle, WriteConsoleW, SetFilePointerEx, SetStdHandle, GetConsoleMode, GetConsoleCP, FlushFileBuffers, lstrcpyA, GetUserDefaultLCID, IsValidLocale, GetLocaleInfoW, LCMapStringW, CompareStringW, GetTimeFormatW, GetDateFormatW, HeapSize, GetStringTypeW, HeapReAlloc, HeapAlloc, WaitForSingleObjectEx, EnumCalendarInfoW, CreateDirectoryW, EnumSystemLocalesW, GlobalFix, OutputDebugStringW, RtlUnwind, LoadLibraryExW, FreeLibrary, GetCommandLineA, GetLastError, SetLastError, GetCurrentThread, GetCurrentThreadId, EncodePointer, DecodePointer, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, WideCharToMultiByte, GetProcessHeap, GetStdHandle, GetFileType, DeleteCriticalSection, GetStartupInfoW, GetModuleFileNameA, WriteFile, GetModuleFileNameW, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetEnvironmentStringsW, FreeEnvironmentStringsW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, InitializeCriticalSectionAndSpinCount, CreateEventW, Sleep, GetCurrentProcess, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetTickCount, GetModuleHandleW, CreateSemaphoreW, EnterCriticalSection, LeaveCriticalSection, FatalAppExitA, HeapFree, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, IsDebuggerPresent, IsProcessorFeaturePresent, SetConsoleCtrlHandler, CreateFileW
MPR.dll	WNetDisconnectDialog1W, WNetGetResourceParentW, WNetGetNetworkInformationW, WNetGetResourceInformationW, WNetAddConnection3A
MSACM32.dll	acmFilterTagEnumA, acmDriverEnum, acmFormatChooseW, acmStreamMessage, acmFilterEnumA, acmFormatEnumW, acmDriverDetailsW, acmFormatSuggest
loadperf.dll	LoadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA, LoadPerfCounterTextStringsA
GDI32.dll	UnrealizeObject, GetGlyphOutline, GetCharABCWidthsFloatW, GetNearestColor
WINSPOOL.DRV	StartDocPrinterW, SetPortW, DEVICECAPABILITIES

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
Nov 27, 2020 02:13:19.684223890 CET	52991	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:19.711155891 CET	53	52991	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:20.495153904 CET	53700	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:20.540332079 CET	53	53700	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:24.369039059 CET	51726	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:24.414710999 CET	53	51726	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:25.298772097 CET	56794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:26.295061111 CET	56794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:27.271684885 CET	53	56794	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:27.289997101 CET	53	56794	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:28.195287943 CET	56534	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:28.240853071 CET	53	56534	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:34.715626955 CET	56627	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:34.761481047 CET	53	56627	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:43.525080919 CET	56621	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:43.552237988 CET	53	56621	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:49.346569061 CET	63116	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:49.392435074 CET	53	63116	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:50.912091970 CET	64078	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:50.939233065 CET	53	64078	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:54.020884037 CET	64801	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:54.066385984 CET	53	64801	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:56.835398912 CET	61721	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:56.862602949 CET	53	61721	8.8.8.8	192.168.2.4
Nov 27, 2020 02:13:58.322797060 CET	51255	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:13:58.368381977 CET	53	51255	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:19.778223991 CET	61522	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:14:19.805511951 CET	53	61522	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:21.833511114 CET	52337	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 02:14:21.880470037 CET	53	52337	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:22.198148966 CET	55046	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:14:22.243976116 CET	53	55046	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:22.772913933 CET	49612	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:14:22.817907095 CET	53	49612	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:54.328602076 CET	49285	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:14:54.355868101 CET	53	49285	8.8.8.8	192.168.2.4
Nov 27, 2020 02:14:59.965514898 CET	50601	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:00.019509077 CET	53	50601	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:01.638467073 CET	60875	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:01.686320066 CET	53	60875	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:42.678425074 CET	56448	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:42.727615118 CET	53	56448	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:43.275799990 CET	59172	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:43.303050995 CET	53	59172	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:43.733561039 CET	62420	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:43.779498100 CET	53	62420	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:44.111159086 CET	60579	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:44.111537933 CET	50183	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:44.138638020 CET	53	50183	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:44.179713964 CET	53	60579	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:44.429959059 CET	61531	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:44.491183996 CET	53	61531	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:44.536788940 CET	49228	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:44.582063913 CET	53	49228	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:45.127212048 CET	59794	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:45.172296047 CET	53	59794	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:45.622747898 CET	55916	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:45.668445110 CET	53	55916	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:46.185383081 CET	52752	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:46.230737925 CET	53	52752	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:47.014724016 CET	60542	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:47.060239077 CET	53	60542	8.8.8.8	192.168.2.4
Nov 27, 2020 02:15:47.505640030 CET	60689	53	192.168.2.4	8.8.8.8
Nov 27, 2020 02:15:47.551796913 CET	53	60689	8.8.8.8	192.168.2.4

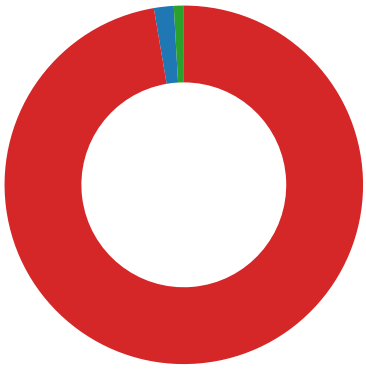
ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 27, 2020 02:13:27.290100098 CET	192.168.2.4	8.8.8.8	d078	(Port unreachable)	Destination Unreachable

Code Manipulations

Statistics

Behavior



💡 Click to jump to process

System Behavior

Analysis Process: INV.exe PID: 6580 Parent PID: 4200

General

Start time:	02:13:24
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\INV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INV.exe'
Imagebase:	0x90000
File size:	394240 bytes
MD5 hash:	83259CB82642666503278233421C306D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.646857656.00000000000B1000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AF781	ReadFile

Analysis Process: conhost.exe PID: 6592 Parent PID: 6580

General

Start time:	02:13:24
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: INV.exe PID: 6640 Parent PID: 6580

General

Start time:	02:13:25
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\INV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INV.exe
Imagebase:	0x90000
File size:	394240 bytes
MD5 hash:	83259CB8264266650327823342 1C306D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000003.645815699.0000000000D26000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000003.645815699.0000000000D26000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000003.645815699.0000000000D26000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.667791715.0000000003915000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.667791715.0000000003915000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.667791715.0000000003915000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.666412273.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.666412273.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.666412273.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile

Analysis Process: WerFault.exe PID: 6752 Parent PID: 6640

General

Start time:	02:13:28
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6640 -s 872
Imagebase:	0x390000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6B901717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6B8F497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp	success or wait	1	6B8F497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	success or wait	1	6B8F4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	success or wait	1	6B8F4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp.xml	success or wait	1	6B8F4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B31.tmp.csv	success or wait	1	6B8F4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5DF1.tmp.txt	success or wait	1	6B8F4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 ba 52 c0 5f a4 05 12 00 00 00 00 00	MDMP..... .....R._.....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.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 f8 1a 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 f0 19 00 00 b5 52 c0 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	.....U.....B..... ..GenuineIntelW.....T... .....R._..... .....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 0b 00 07 80 00 d8 02 00 20 d0 ce 00 00 00 cd 00 ee b7 2c e3 12 4b b9 e3 fc fc 95 00 7e b6 e3 76 23 00 00 00 06 02 01 00 f0 fc 95 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........... ....,..K.. ....~..v#...........+.........	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	168	f4 19 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 7e b6 e3 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 d8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 7a 1f 00 00	........................~..v.. ....z...	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	20	bc 00 00 00 00 e0 72 00 00 00 00 00 00 10 00 00 06 3c 00 00	......r..........<..	success or wait	188	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	4096	0c fc a0 04 00 00 a1 04 00 e0 a0 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 e0 72 00 00 00 00 00 f0 19 00 00 10 1a 00 00 00 00 00 00 f8 80 cd 00 00 f0 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........................r... ....q......... ....p.w.............	success or wait	187	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	4096	40 f7 87 02 00 00 88 02 00 e0 87 02 00 00 00 00 00 1e 00 00 00 00 00 00 00 b0 72 00 00 00 00 00 f0 19 00 00 0c 1a 00 00 00 00 00 00 a8 80 cd 00 00 f0 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@.........................r... ....q......... ....p.w.............	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 88 ee 95 00 bc 9a 11 77 23 00 00 00 02 02 00 00 f8 ec 95 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#...........+.........	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	48	10 1a 00 00 01 00 00 00 20 00 00 00 02 00 00 00 00 e0 72 00 00 00 00 00 a8 fb a0 04 00 00 00 00 58 04 00 00 ee 81 00 00 cc 02 00 00 76 2d 00 00	....r........... ..X...........v-..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	4	27 00 00 00	'...	success or wait	39	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	20	0e 00 00 00 49 00 4e 00 56 00 2e 00 65 00 78 00 65 00 00 00	....I.N.V...e.x.e...	success or wait	39	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	752	00 00 71 76 00 00 00 00 00 70 04 00 e6 eb 04 00 f8 ac 1a 38 5c 1f 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 ba 02 00 00 00 00 00 a0 2f 03 00 00 00 00 a3 54 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 7c 69 03 00 00 00 00 00 ae 73 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 3c 1b 00 00 00 00 00 a4 c2 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 3d d3 04 00 00 00 00	..qv.....p.........8\......... ....B.......B?........... ....%............ ..@A..................Zb...... ....`........./..... .T..................|i.......s ....<............. @.......=......	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	14064	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C8.tmp.dmp	unknown	108	03 00 00 00 f4 00 00 00 fc 06 00 00 04 00 00 00 78 10 00 00 fc 07 00 00 05 00 00 00 c4 0b 00 00 42 30 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 98 22 00 00 32 82 01 00 15 00 00 00 ec 01 00 00 74 18 00 00 16 00 00 00 98 00 00 00 60 1a 00 00	.....x.....B0.....T.....8.....T.....".."..2.....t.....`...	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.4.0.<./.P.i.d.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 49 00 4e 00 56 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.>.I.N.V...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 32 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.6.2.2.<./.U.p.t.i.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 34 00 38 00 35 00 33 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.5.4.8.5.3.3.7.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 34 00 38 00 34 00 35 00 31 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.>.1.5.4.8.4.5.1.8.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 33 00 38 00 33 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.8.3.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	98	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 34 00 39 00 30 00 31 00 32 00 34 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.>.1.4.9.0.1.2.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	82	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 34 00 39 00 30 00 31 00 32 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.9.0.1.2.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 32 00 32 00 36 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.6.4.6.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 32 00 32 00 36 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.6.2.9.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 33 00 32 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.3.2.0.7.2.<./.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 33 00 31 00 38 00 30 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.>.3.1.8.0.0.<./.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 36 00 35 00 39 00 38 00 36 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.9.8.6.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 36 00 37 00 37 00 34 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.7.7.4.7.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 36 00 35 00 39 00 38 00 36 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.5.9.8.6.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.5.8.0.<./.P.i.d.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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.>.(.u.n.a.b.l.e. .t.o. .r.e.t.r.i.e.v.e.).<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 34 00 35 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.>.6.4.5.5.<./.U.p.t.i.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 35 00 39 00 30 00 32 00 33 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.9.0.2.3.3.6.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	56	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 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 36 00 38 00 31 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.6.8.1.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	98	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 30 00 30 00 34 00 37 00 34 00 38 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.>.1.0.0.4.7.4.8.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	76	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 32 00 30 00 34 00 38 00 30 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.>.2.0.4.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 30 00 38 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.8.4.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	88	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 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	122	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 39 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.9.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	100	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 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.>.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	72	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 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 34 00 38 00 37 00 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.4.8.7.0.1.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	68	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 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 49 00 4e 00 56 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.>.I.N.V...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 72 00 71 00 79 00 73 00 6f 00 71 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.>.r.q.y.s.o.q.,. .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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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 72 00 71 00 79 00 73 00 6f 00 71 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.>.r.q.y.s.o.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 38 00 31 00 38 00 35 00 30 00 34 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.8.1.8.5.0.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	70	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 2d 00 30 00 31 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.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 30 00 2d 00 31 00 31 00 2d 00 32 00 37 00 54 00 30 00 31 00 3a 00 31 00 33 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.1.-.2.7.T.0.1.:.1.3.:.3.1.Z.".>.	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	262	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 35 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 36 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 36 00 32 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 36 00 32 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.1.". .P.I.D.=.".6.6.4.0.". .U.p.t.i.m.e.M.S.=.".1.6.2.4. ". .T.i.m.e.S.i.n.c.e.C.r.e.a. t.i.o.n.M.S.=.".1.6.2.4.". .S. u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 36 00 63 00 66 00 30 00 35 00 34 00 35 00 2d 00 31 00 36 00 64 00 31 00 2d 00 34 00 66 00 65 00 34 00 2d 00 39 00 61 00 37 00 38 00 2d 00 33 00 32 00 35 00 38 00 63 00 33 00 65 00 34 00 30 00 63 00 64 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.6.c.f.0.5.4.5.-.1.6.d.1.-.4.f.e.4.-.9.a.7.8.-.3.2.5.8.c.3.e.4.0.c.d.6.<./.G.u.i.d.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 30 00 2d 00 31 00 31 00 2d 00 32 00 37 00 54 00 30 00 31 00 3a 00 31 00 33 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.1.-.2.7.T.0.1.:.1.3.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597C.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	6B8F497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B13.tmp.xml	unknown	4533	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15\Report.wer	unknown	2	ff fe	..	success or wait	1	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15\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	169	6B8F497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_INV.exe_7fa5c1fc50c97be82372a0bb1297551a3548ed7_49edae5c_1a096a15\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 39 00 37 00 30 00 37 00 38 00 35 00 31 00 34 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.9.7.0.7.8.5.1.4.1.	success or wait	1	6B8F497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	success or wait	1	6B9136BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6B911FB2	RegCreateKeyExW
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6B8F43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	ProgramId	unicode	000669d35ae915c2c96fc6d36ce528802e4b0000ffff	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	FileId	unicode	0000180e81bab341eda0d404b8f5fed93bc3b350cfbd	success or wait	1	6B9136BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	LowerCaseLongPath	unicode	c:\users\user\desktop\inv.exe	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	LongPathHash	unicode	inv.exe|f352b40e	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	Name	unicode	inv.exe	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	Publisher	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	Version	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	BinFileVersion	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	BinaryType	unicode	pe32_i386	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	ProductName	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	ProductVersion	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	LinkDate	unicode	11/26/2020 22:54:37	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	BinProductVersion	unicode		success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	Size	B	00 04 06 00 00 00 00 00	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	Language	dword	0	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	IsPeFile	dword	1	success or wait	1	6B9136BF	unknown
\REGISTRY\A\{4c3ee17e-3381-fdfe-1e45-765618f1cf85}\Root\InventoryApplicationFile\inv.exe|f352b40e	IsOsComponent	dword	0	success or wait	1	6B9136BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 7E B6 E3 76 02 00 00 00 00 00 00 00 08 D8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6B911FE8	RegSetValueExW

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

Disassembly

Code Analysis