ID: 339364
Sample Name: FYI.exe
Cookbook: default.jbs
Time: 21:41:53
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

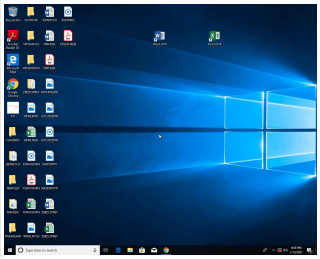
Analysis Report FYI.exe

Overview

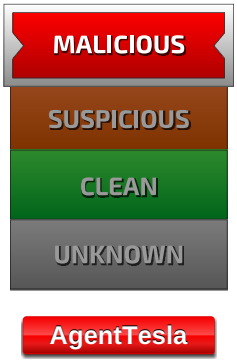
General Information

Sample Name:	FYI.exe
Analysis ID:	339364
MD5:	4768fad22f989c9..
SHA1:	78f2e47fbcd50d7..
SHA256:	275b79db451178..
Tags:	exe

Most interesting Screenshot:



Detection

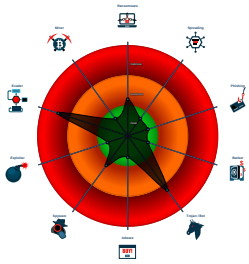


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Detected potential crypto function
- May sleep (evasive loops) to hinder …
- Monitors certain registry keys / valu…
- One or more processes crash
- PE file contains strange resources
- Queries the volume information (nam…
- Sample file is different than original

Classification



Startup

- **System is w10x64**
- FYI.exe (PID: 7132 cmdline: 'C:\Users\user\Desktop\FYI.exe' MD5: 4768FAD22F989C9AC940775CA46F91F6)
  - WerFault.exe (PID: 4832 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7132 -s 1160 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

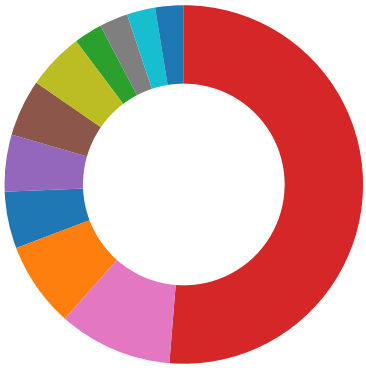
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.415958937.000000000266 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.416956383.000000000366 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: FYI.exe PID: 7132	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: FYI.exe PID: 7132	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

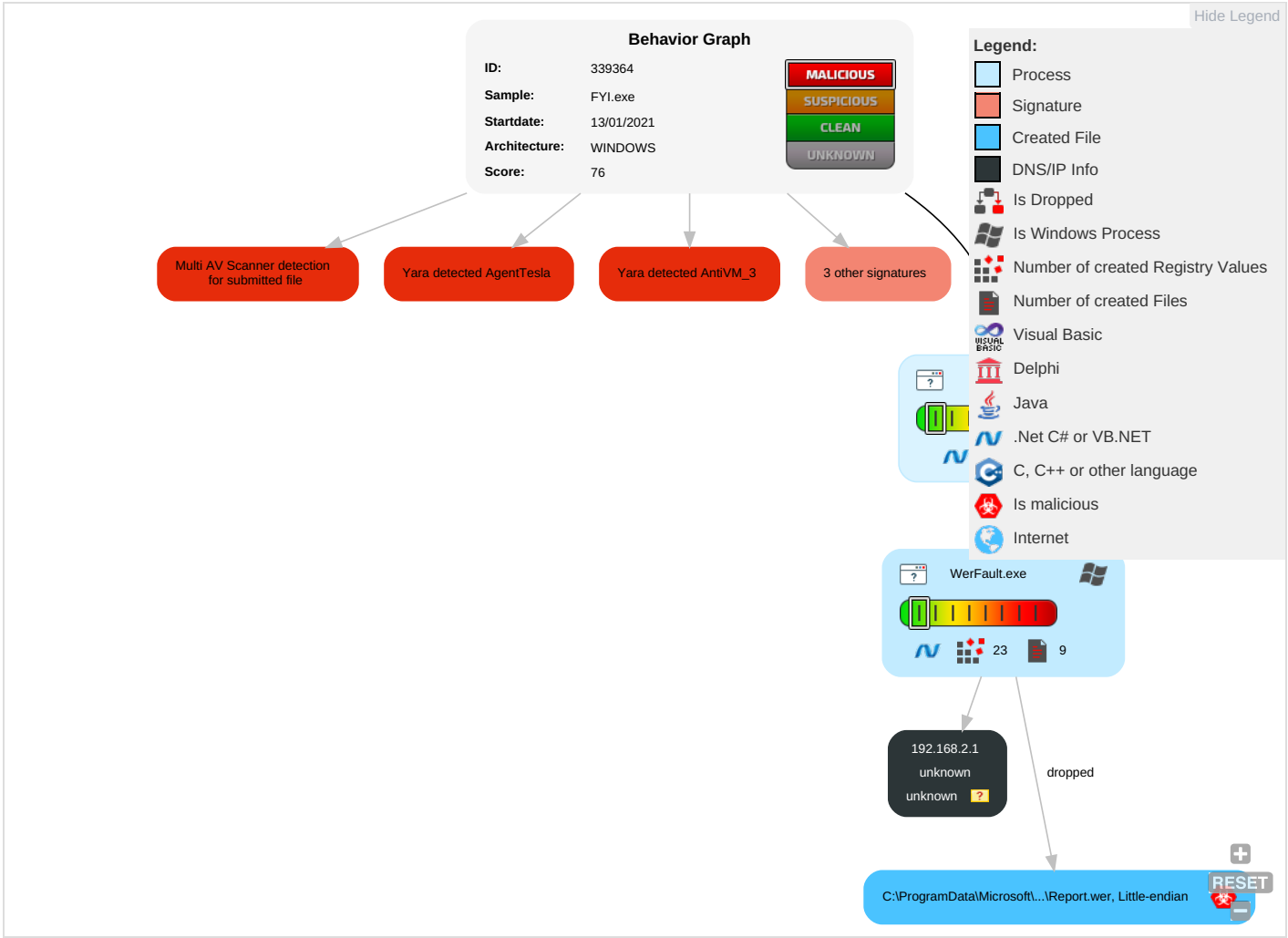
Yara detected AgentTesla

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

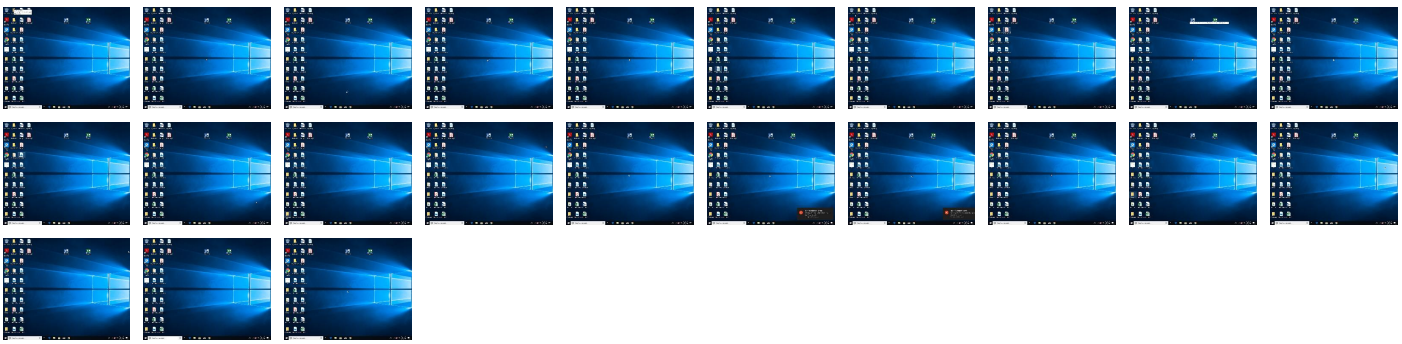
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FYI.exe	28%	Virustotal		Browse
FYI.exe	13%	ReversingLabs	Win32.Trojan.Generic	
FYI.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

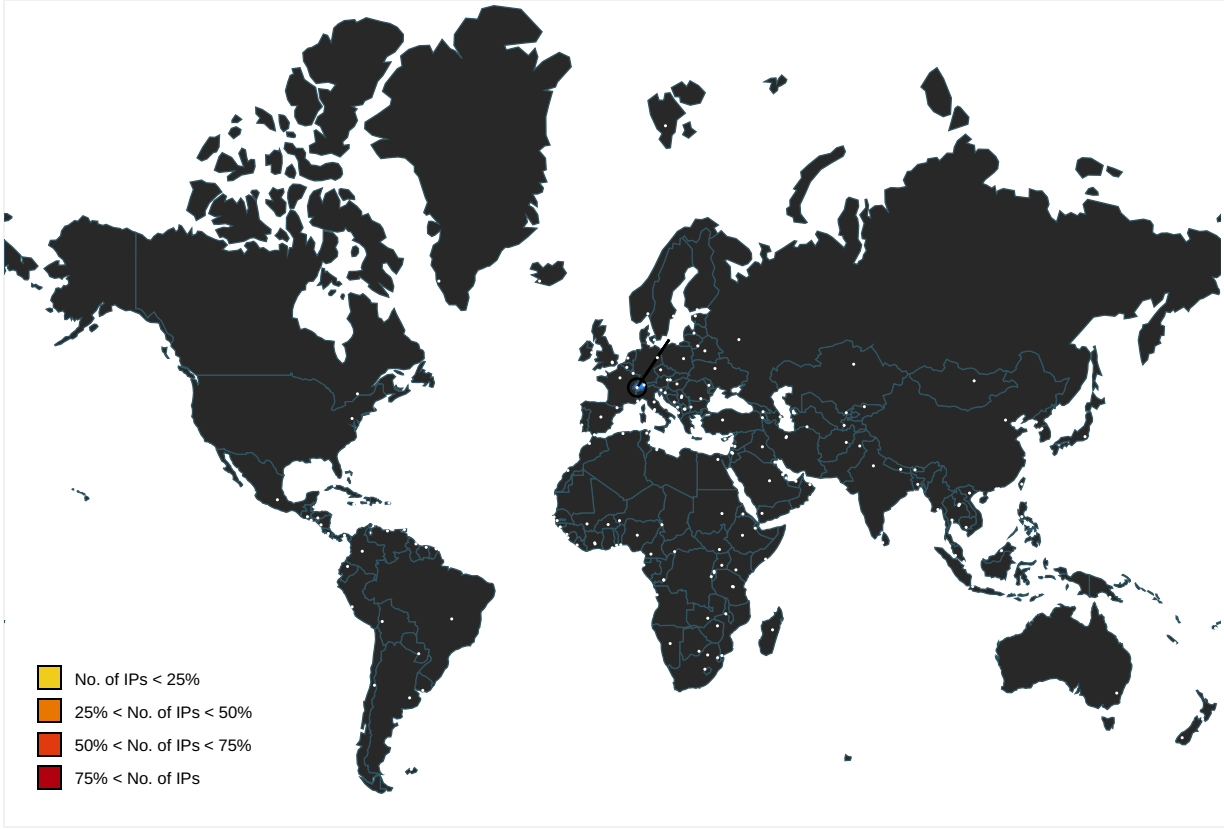
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthrhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddressxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	FYI.exe, 00000000.00000002.416956383.0000000003669000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000004.00000003.358763831.0000000004FE0000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339364
Start date:	13.01.2021
Start time:	21:41:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FYI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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:	mal76.troj.evad.winEXE@2/4@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 51.104.139.180, 92.122.213.194, 92.122.213.247, 168.61.161.212, 93.184.221.240, 51.103.5.159, 20.54.26.129, 52.155.217.156, 23.210.248.85 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:42:52	API Interceptor	1x Sleep call for process: FYI.exe modified
21:43:18	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14450
Entropy (8bit):	3.771478576899414
Encrypted:	false
SSDEEP:	192:nWNnkgHBUZMXqaKeCiynKz/u7sCS274ItM7:WNnLBUZMXqav/u7sCX4ItM7
MD5:	19C943447658E2C23D5AE333BA6CC6E9
SHA1:	EAFE017FC8DB5497D1026188C9C16D08E242E88F
SHA-256:	9082B7E39BF17FC2F26A834C7A2E9898906B4C706ABCDB19967DB7E364FAE8E8
SHA-512:	CE7E65A665B350D1AE8B7E0521225EB435EE5CE76B35C8BC8F7B3B5EDAAD29C89B716317545A92C4D57C88A91217D6CB0C1C69503C3BACF50433EC48AFCB2DC
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.7.6.5.7.6.7.8.1.8.0.8.5.....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.=.1.3.2.5.5.0.7.6.5.8.3.3.2.8.6.4.9.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.0.7.1.5.4.9.9.-.a.1.9.a.-.4.9.e.6.-.b.4.a.1.-.8.6.a.8.b.c.f.2.6.e.9.d.....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.=.1.e.c.9.8.3.9.1.-.a.4.c.8.-.4.4.e.5.-.8.2.2.7.-.b.5.1.4.f.3.4.9.4.a.a.5.....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.=.F.Y.I...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.E.L.E.M.D.E.S.C...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.d.c.-.0.0.0.1.-.0.0.1.7.-.8.7.0.4.-.8.c.1.6.3.8.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.a.5.6.1.8.9.0.8.5.5.9.0.7.6.5.f.e.8.8.b.c.a.2.8.e.0.e.8.6.d.8.0.0.0.0.0.0.0.0.!.0.0.0.0.7.8.f.2.e.4.7.f.b.c.d.5.0.d.7.7.b.8.c.0.e.a.5.e.0.7.2.0.9.a.2.b.1.a.7.9.c.4.5.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jan 14 05:42:58 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	268581
Entropy (8bit):	4.473454946615885
Encrypted:	false
SSDEEP:	3072:V0A9UCgUrU9gIOgF5YvVm1oiwyMHEEI0lCR1EO0jd+pSabt7:VnTj49RpDYs1j+I0lCR9pS8
MD5:	691D98FD805127129A2CAC03D6C32AB4
SHA1:	C5C8D660EC5DAFBC973FF31100B10DD141C89834
SHA-256:	BDF5DC92ACD40D607BA423EA47B1C2EF54A03F782572E5D0FA0FE025D7C01849
SHA-512:	B24108C751D560C5663AEEF4111B083014692A15E8D43ACF30335E11C7C7B6B94D54595128FF0C8DA5E8218B639825EC1E454D15FEE32A56F87D33DF16AE1345
Malicious:	false
Reputation:	low
Preview:	MDMP..... ....._.....U.....B....."....GenuineIntelW.....T....._.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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):	8374
Entropy (8bit):	3.69482804710006

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiQZ6h6YJrSUIFlggmfZfSdCprF89bYRsfc+om:RrlsNi26h6YVSUIFigmfBSnYKfcY
MD5:	91110FF09C7FC442779F7EF580769F22
SHA1:	57C9D5D4865F64BE2ED5A5E5EA629449D9482287
SHA-256:	56ECD21B10ED2EC7F9BDC0358279EBC0222EC5B50ACD51C7ED0FCE0D1837284F
SHA-512:	4D69FD3214085D778645788B591FE49B00272AD667B3EA2222FBA895DDFCC3D6F3A1E194A7ECBCCAA9D6A691FC64FEFBAD3744F2251B60303BB02F5AAE7127 0
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.>.7.1.3.2.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4703
Entropy (8bit):	4.452410891996699
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9yMWSC8Bz8fm8M4J0eH2FC+q8vOeHmHwbeOCd:uITfftlSNeJLK2Hiend
MD5:	A8539EC6F218065D2C5A263606E75913
SHA1:	F1B63F2D4B25EC3C75BA64C5F856F302947D4E33
SHA-256:	5CBFED0D236862A5F0BAD8621CCB4BDAD446DB68F61EF6C21837EE21B1735EB6
SHA-512:	63825E3006D33D138C1553043B397751F83FFD8456C4B2FF0DA870D8133CE151C0F6093B495D89A858EF7036AB3AB9C3BC8545D8910385B4114700449720CD74
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="815933" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.0302421461740785
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	FYI.exe
File size:	930816
MD5:	4768fad22f989c9ac940775ca46f91f6
SHA1:	78f2e47fbcd50d77b8c0ea5e07209a2b1a79c45e
SHA256:	275b79db451178b96e4872f9164b8b89f25a5f22ff8ba5f9 83d555cb3972a95d
SHA512:	74d822b0b1374af9f53b603c145a58482b843aab9fcab43 f1c64cc7c4ab6d189998d1964ad2e300d52f124d827175a aea3e3f78a836d07906a703997b5a8ad52
SSDEEP:	12288:RK+ympVh1Iw6lLkTYBt12mS0E4h9gwi4z3d87O GMA:aQVUxl6YBtr51iI3d87LMA
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L...h .._.....P..J.....i... .....@.. ....@.....

File Icon

Icon Hash:	000d233320000000

Static PE Info

General

Entrypoint:	0x4c691a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEC368 [Wed Jan 13 09:54:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc68c8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x1e43c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	0xc	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc4920	0xc4a00	False	0.684223269628	data	7.25136431131	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x1e43c	0x1e600	False	0.268614969136	data	3.13907628015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc8220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xc8688	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294901502, next used block 4294901501		
RT_ICON	0xc9730	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294704636, next used block 4294704380		
RT_ICON	0xcbcd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294573050, next used block 4294638330		
RT_ICON	0xcff00	0x10828	data		
RT_ICON	0xe0728	0x5797	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xe5ec0	0x5a	data		
RT_VERSION	0xe5f1c	0x334	data		
RT_MANIFEST	0xe6250	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	ELEMDESC.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement

Description	Data
ProductVersion	1.0.0.0
FileDescription	FileReplacement
OriginalFilename	ELEMDESC.exe

Network Behavior

UDP Packets

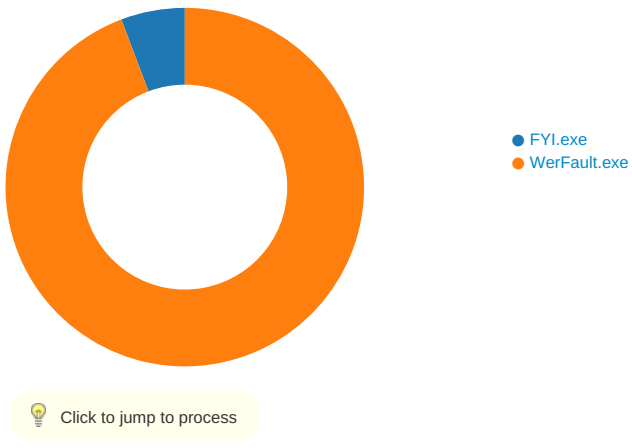
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:42:56.448657990 CET	64267	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:42:56.496658087 CET	53	64267	8.8.8.8	192.168.2.6
Jan 13, 2021 21:42:58.081685066 CET	49448	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:42:58.132519007 CET	53	49448	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:04.604155064 CET	60342	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:04.655970097 CET	53	60342	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:10.414232969 CET	61346	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:10.462306976 CET	53	61346	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:17.180489063 CET	51774	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:17.238306999 CET	53	51774	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:19.978152037 CET	56023	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:20.026010036 CET	53	56023	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:23.018889904 CET	58384	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:23.066829920 CET	53	58384	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:25.248848915 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:25.296953917 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:26.403151989 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:26.451338053 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:27.410645008 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:27.461308002 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:28.361809969 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:28.410039902 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:29.513449907 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:29.564551115 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:30.486542940 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:30.537297964 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:30.669805050 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:30.717756033 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:31.732527018 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:31.783268929 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:32.202323914 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:32.258920908 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:33.146409988 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:33.197583914 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:35.430470943 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:35.486900091 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:36.609778881 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:36.657830000 CET	53	63307	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:37.779505014 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:37.831496954 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:37.985586882 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:38.044173002 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:39.084952116 CET	50010	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:39.132936954 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:40.273437023 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:40.325709105 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:41.292197943 CET	62116	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:41.340086937 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:46.599957943 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:46.668344975 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:46.676014900 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:46.727622986 CET	53	55014	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:43:47.335315943 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:47.399907112 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:48.047955990 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:48.096183062 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:48.557751894 CET	51818	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:48.616976976 CET	53	51818	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:49.063502073 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:49.121870041 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:49.651891947 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:49.710367918 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:50.277299881 CET	53799	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:50.339318991 CET	53	53799	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:51.072112083 CET	54683	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:51.129157066 CET	53	54683	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:52.179287910 CET	59329	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:52.236133099 CET	53	59329	8.8.8.8	192.168.2.6
Jan 13, 2021 21:43:52.765718937 CET	64021	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:43:52.822047949 CET	53	64021	8.8.8.8	192.168.2.6
Jan 13, 2021 21:44:13.033729076 CET	56129	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:44:13.089921951 CET	53	56129	8.8.8.8	192.168.2.6
Jan 13, 2021 21:44:14.236213923 CET	58177	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:44:14.294318914 CET	53	58177	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: FYI.exe PID: 7132 Parent PID: 5888

General

Start time:	21:42:47
Start date:	13/01/2021

Path:	C:\Users\user\Desktop\FYI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FYI.exe'
Imagebase:	0x1a0000
File size:	930816 bytes
MD5 hash:	4768FAD22F989C9AC940775CA46F91F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.415958937.0000000002661000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.416956383.0000000003669000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0CCF06	unknown

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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E08D72F	unknown
C:\Users\user\Desktop\FYI.exe	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Users\user\Desktop\FYI.exe	unknown	512	success or wait	1	6E08D72F	unknown

Analysis Process: WerFault.exe PID: 4832 Parent PID: 7132

General

Start time:	21:42:54
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7132 -s 1160
Imagebase:	0x9d0000
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	6AC81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6AC7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	success or wait	1	6AC74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	success or wait	1	6AC74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp.xml	success or wait	1	6AC74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8340.tmp.csv	success or wait	1	6AC74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86BC.tmp.txt	success or wait	1	6AC74BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 e2 d9 ff 5f a4 05 12 00 00 00 00 00	MDMP........ ...._........	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.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 c0 22 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 dc 1b 00 00 d7 d9 ff 5f 02 00 00 00 01 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 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B.......".... ..GenuineIntelW...........T... ...._................. ....0................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.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 01 00 00 00 a0 ea 6f 00 05 00 00 00 00 00 00 00 05 00 00 00 e0 e9 6f 00 38 ea 6f 00 22 d7 bb 76 23 00 00 00 12 02 20 00 e0 e9 6f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.........o..............o. 8.o."..v#..... ...o.+.........	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	168	e0 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 bb 76 00 00 00 00 05 00 00 00 00 00 00 00 09 15 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 6d 00 00 00 00 20 0d 78 00 00 00 00 00 f4 ea 6f 00 00 00 00 00 01 00 00 00 00 00 00 00 50 ea 6f 00 00 00 00 00 00 a3 2c fd 6d 00 00 00 00 9f 2a c1 ee ff ff ff ff 70 4f 7d 00 00 00 00 00 10 a7 7b 05 00 00 00 00 40 0f 62 05 00 00 00 00 00 ea 6f 00 00 00 00 00 00 cc 02 00 00 84 29 00 00	........RCC.....".v.. ....m.... .x..... o.....P.o.....,.m.... .*.....pO}.....{.....@.b... ....o.....)..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	20	89 03 00 00 b8 ac b4 6c 00 00 00 00 b8 28 00 00 ac 75 00 00	.....l.....(...u..	success or wait	905	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	10424	01 00 00 00 00 00 00 00 03 00 00 00 11 8a 40 00 07 00 00 00 5d de 42 00 09 00 00 00 fd 71 43 00 0e 00 00 00 99 54 40 00 0f 00 00 00 4d 71 43 00 10 00 00 00 49 ff 44 00 11 00 00 00 85 c0 40 00 12 00 00 00 cd ff 44 00 13 00 00 00 11 8f 43 00 14 00 00 00 91 f7 41 00 15 00 00 00 b1 ec 41 00 16 00 00 00 e5 c0 40 00 17 00 00 00 15 c1 40 00 1a 00 00 00 a1 54 40 00 21 00 00 00 85 7a 40 00 22 00 00 00 15 37 40 00 23 00 00 00 19 ed 44 00 24 00 00 00 71 ec 44 00 25 00 00 00 b9 ec 44 00 26 00 00 00 d1 25 45 00 31 00 00 00 4d 4e f6 ff 39 00 00 00 f1 ac 44 00 3a 00 00 00 8d f8 44 00 3b 00 00 00 a5 f9 44 00 3c 00 00 00 d9 f7 44 00 3d 00 00 00 99 2a 40 00 3f 00 00 00 55 bf 44 00 40 00 00 00 61 d6 44 00 41 00 00 00 a5 c4 44 00 42 00 00 00 11 db 44 00 43 00 00 00 d1 01 45	.....@.....].B.....q C.....T@.....MqC.....I.D..... ..@.....D.....C.....A... ....A.....@.....@.....T@. !....z@."....7@.#.....D.$...q. D.%.....D.&....%E.1...MN..9 .....D.:.....D.;.....D.<.....D.=. ...*@.?...U.D.@...a.D.A..... D.B.....D.C.....E	success or wait	904	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	8	f3 00 00 00 1b 01 00 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	4	06 00 00 00	....	success or wait	6	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 78 db 6f 00 bc 9a e5 77 23 00 00 00 06 02 20 00 e8 d9 6f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+.......................... x.o....w#..... ...o.+.........	success or wait	6	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	48	d4 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 d0 47 00 00 00 00 00 ac fa f5 04 00 00 00 00 54 05 00 00 e6 81 01 00 cc 02 00 00 4c 3a 00 00	....G........... ..T...........L:..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	4	39 00 00 00	9...	success or wait	57	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	20	0e 00 00 00 46 00 59 00 49 00 2e 00 65 00 78 00 65 00 00 00	....F.Y.I...e.x.e...	success or wait	57	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	752	00 00 f0 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 5e 29 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 a0 02 00 00 00 00 00 10 c6 02 00 00 00 00 7d 46 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 72 03 00 00 00 00 00 99 74 03 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 45 1b 00 00 00 00 00 25 ba 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00	...j.............`.Z^)........ ....?........... ....)............. ..@A..................Zb...... ....P............. }F..................@r.......t ....E......%....... @..............	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	18518	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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7630.tmp.dmp	unknown	108	03 00 00 00 24 01 00 00 fc 06 00 00 04 00 00 00 10 18 00 00 2c 08 00 00 05 00 00 00 94 38 00 00 18 3d 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 88 2d 00 00 e5 eb 03 00 15 00 00 00 ec 01 00 00 3c 20 00 00 16 00 00 00 98 00 00 00 28 22 00 00	....$.....,.....8...=.....T.....8.....T.....-.....<.....("...	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.3.2.<./.P.i.d.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 46 00 59 00 49 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.>.F.Y.I ...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u .r.e.>.0.0.0.0.0.0.0.0. <./.C.m. d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 33 00 34 00 39 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.>.1.2.3.4.9. <./.U.p.t.i.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 32 00 30 00 33 00 36 00 36 00 35 00 34 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.0.3.6.6.5.4.0.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 32 00 30 00 33 00 36 00 35 00 37 00 32 00 31 00 36 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.>.2.0.3.6.5.7.2.1.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 37 00 32 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.7.2.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 33 00 38 00 38 00 35 00 30 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.8.5.0.5.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 33 00 38 00 38 00 35 00 30 00 35 00 36 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.>.3.8.8.5.0.5.6.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 33 00 31 00 39 00 33 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.9.3.3.6.<./.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 33 00 31 00 39 00 33 00 33 00 33 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.>.3.1.9.3.3.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 32 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.4.2.1.9.2.<./.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 31 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.4.1.9.2.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 31 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.9.1.2.4.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 38 00 34 00 32 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.8.4.2.2.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 31 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.9.1.2.4.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 30 00 34 00 30 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	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 39 00 31 00 39 00 37 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.1.9.1.9.7.1.<./.U.p.t.i.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 39 00 37 00 36 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.9.7.6.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 38 00 36 00 30 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.8.6.0.5.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 34 00 35 00 39 00 31 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.4.5.9.1.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 31 00 32 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 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.1.2.9.6.<./.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	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 35 00 34 00 35 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.>.9.4.5.4.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.1.0.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 31 00 34 00 30 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.4.1.4.0.1.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 39 00 35 00 37 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.9.5.7.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 31 00 34 00 30 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.4.1.4.0.1.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 46 00 59 00 49 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.>.F.Y.I...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 66 00 70 00 77 00 63 00 6b 00 64 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.>.f.p.w.c.k.d.,. .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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 66 00 70 00 77 00 63 00 6b 00 64 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.>.f.p.w.c.k.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 32 00 37 00 36 00 36 00 32 00 31 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.7.6.6.2.1.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 31 00 34 00 54 00 30 00 35 00 3a 00 34 00 32 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.1.4.T.0.5.:.4.2.:.5.9.Z.".>.	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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 34 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 33 00 32 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 36 00 34 00 39 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 34 00 39 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.9.". .P.I.D.=.".7.1.3.2.". .U.p.t.i.m.e.M.S.=.".6.4.9.9. ". .T.i.m.e.S.i.n.c.e.C.r.e.a. t.i.o.n.M.S.=.".6.4.9.9.". .S. u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 30 00 37 00 31 00 35 00 34 00 39 00 39 00 2d 00 61 00 31 00 39 00 61 00 2d 00 34 00 39 00 65 00 36 00 2d 00 62 00 34 00 61 00 31 00 2d 00 38 00 36 00 61 00 38 00 62 00 63 00 66 00 32 00 36 00 65 00 39 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.0.7.1.5.4.9.9.-.a.1.9.a.-.4.9.e.6.-.b.4.a.1.-.8.6.a.8.b.c.f.2.6.e.9.d.<./.G.u.i.d.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 31 00 34 00 54 00 30 00 35 00 3a 00 34 00 32 00 3a 00 35 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.1.4.T.0.5.:.4.2.:.5.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8053.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	6AC7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8342.tmp.xml	unknown	4703	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	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f\Report.wer	unknown	2	ff fe	..	success or wait	1	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f\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	190	6AC7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_FYI.exe_decd39a630c9d4191a275eb268c8ae351d3d61e4_41043005_12becc4f\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 36 00 36 00 37 00 31 00 31 00 35 00 30 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.6.6.7.1.1.5.0.0.	success or wait	1	6AC7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	success or wait	1	6AC936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6AC91FB2	RegCreateKeyExW
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6AC743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	ProgramId	unicode	0006ca56189085590765fe88bca28e0e86d800000000	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	FileId	unicode	000078f2e47fbcd50d77b8c0ea5e07209a2b1a79c45e	success or wait	1	6AC936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	LowerCaseLongPath	unicode	c:\users\user\desktop\fyi.exe	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	LongPathHash	unicode	fyi.exe|83cd469	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	Name	unicode	fyi.exe	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	Publisher	unicode		success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	Version	unicode	1.0.0.0	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	BinFileVersion	unicode	1.0.0.0	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	BinaryType	unicode	pe32_clr_32	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	ProductName	unicode	filereplacement	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	ProductVersion	unicode	1.0.0.0	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	LinkDate	unicode	01/13/2021 09:54:48	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	BinProductVersion	unicode	1.0.0.0	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	Size	B	00 34 0E 00 00 00 00 00	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	Language	dword	0	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	IsPeFile	dword	1	success or wait	1	6AC936BF	unknown
\REGISTRY\A\{f31b2e32-6810-cc71-36d5-b3d69ebcdb6d}\Root\InventoryApplicationFile\fyi.exe|83cd469	IsOsComponent	dword	0	success or wait	1	6AC936BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 BB 76 05 00 00 00 09 15 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F3 6D 20 0D 78 00 F4 EA 6F 00 01 00 00 00 50 EA 6F 00 A3 2C FD 6D 9F 2A C1 EE 70 4F 7D 00 10 A7 7B 05 40 0F 62 05 00 EA 6F 00	success or wait	1	6AC91FE8	RegSetValueExW

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

Disassembly

Code Analysis