ID: 356249
Sample Name: Invoice 6500TH21Y5674.exe
Cookbook: default.jbs
Time: 20:12:24
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

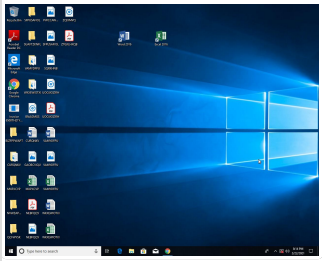
Analysis Report Invoice 6500TH21Y5674.exe

Overview

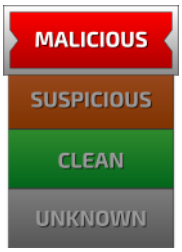
General Information

Sample Name:	Invoice 6500TH21Y5674.exe
Analysis ID:	356249
MD5:	dc22d7783144cfe..
SHA1:	65d3e4f4df34bb2..
SHA256:	c9fc9a54366452a..
Tags:	exe

Most interesting Screenshot:



Detection

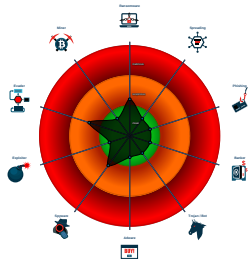


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains capabilities to detect virtua…
- Contains functionality for read data f…
- Contains functionality to access load…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Contains functionality to shutdown / …
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- Invoice 6500TH21Y5674.exe (PID: 7052 cmdline: 'C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe' MD5: DC22D7783144CFE4DCBB4734ED6A3656)
  - WerFault.exe (PID: 1320 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7052 -s 740 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

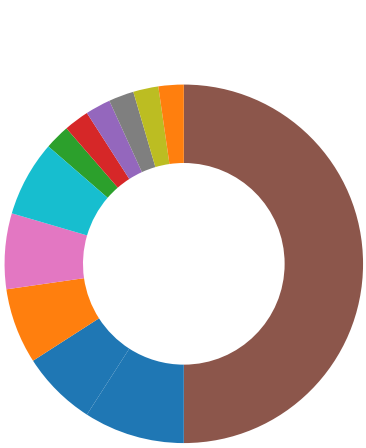
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

System Summary:

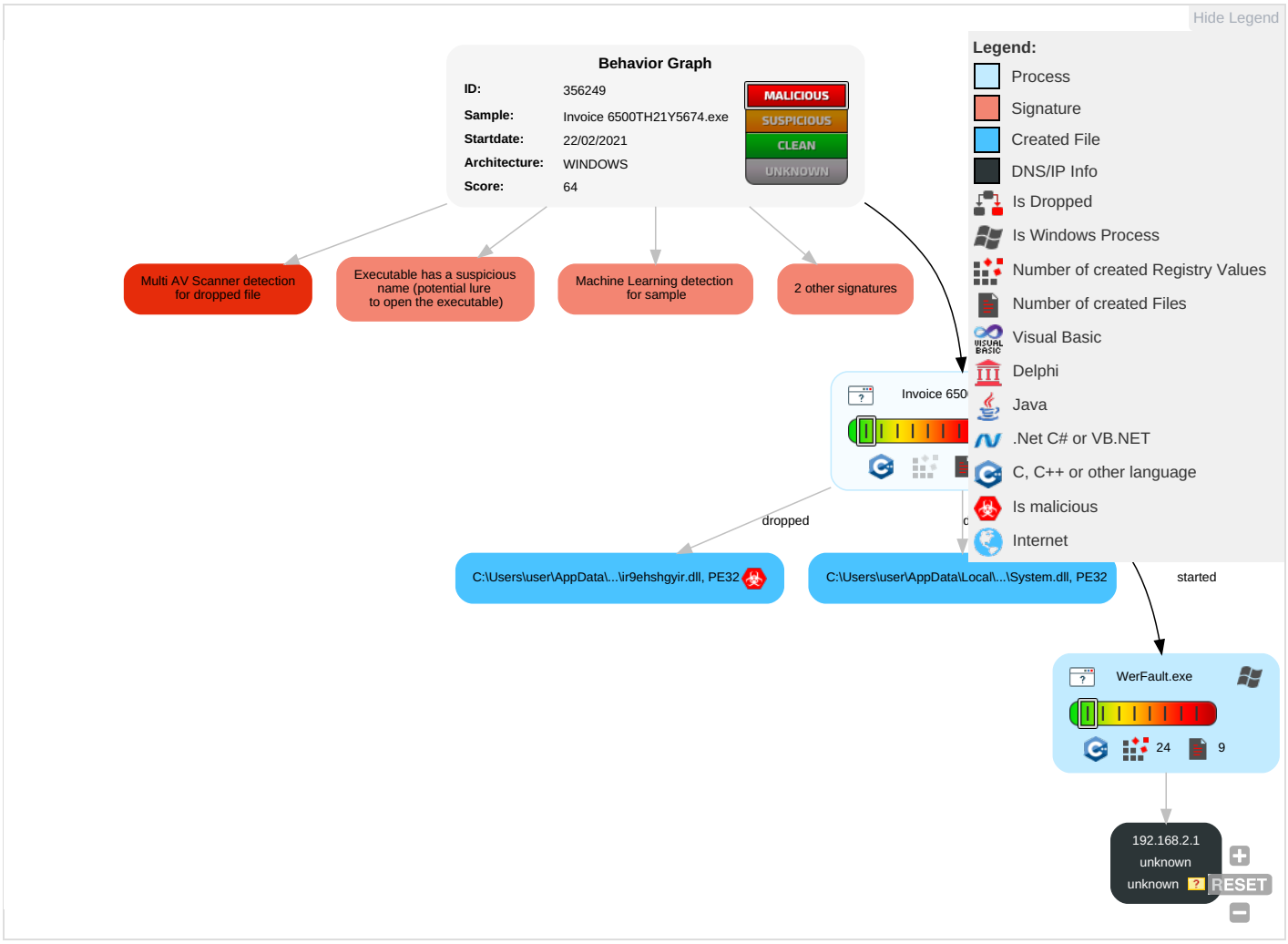
Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Native API 1	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 3	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
Invoice 6500TH21Y5674.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	33%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	29%	ReversingLabs	Win32.Trojan.Convagent	
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

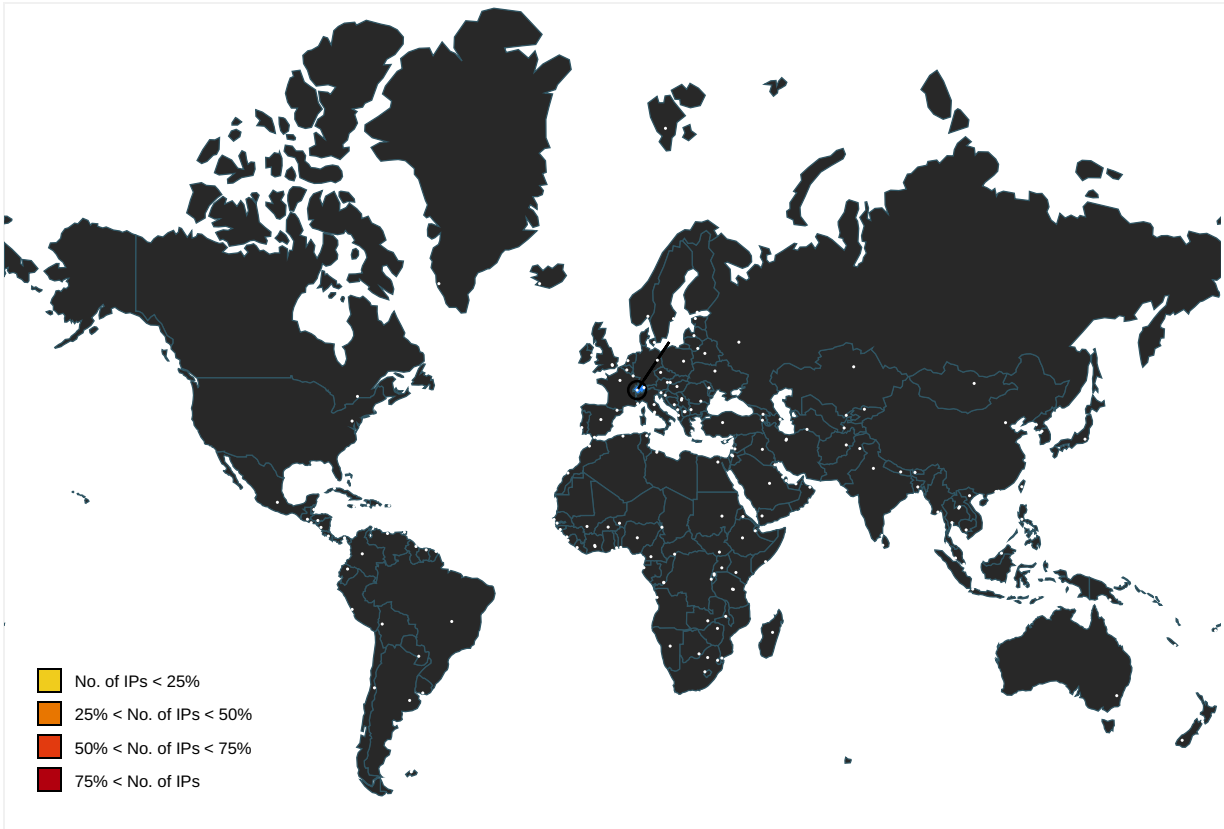
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	Invoice 6500TH21Y5674.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Invoice 6500TH21Y5674.exe	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 Emerald

Analysis ID:	356249
Start date:	22.02.2021
Start time:	20:12:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice 6500TH21Y5674.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:	19
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:	mal64.winEXE@2/7@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 83% (good quality ratio 81.9%) • Quality average: 87.4% • Quality standard deviation: 21.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 184.30.21.144, 51.104.144.132, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
20:13:26	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	GPP.exe	Get hash	malicious	Browse	
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	
	ACCOUNT DETAILS.exe	Get hash	malicious	Browse	
	Quotation.com.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	QuotationInvoices.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.24882.exe	Get hash	malicious	Browse	
	PDF_doc.exe	Get hash	malicious	Browse	
	09000000000000.jar	Get hash	malicious	Browse	
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	
	notice of arrivalpdf.exe	Get hash	malicious	Browse	
	R5BNZ68i0f.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	
	notice of arrival.xlsx	Get hash	malicious	Browse	
	Invoice Overdue.exe	Get hash	malicious	Browse	
	Invoice Overdue.exe	Get hash	malicious	Browse	
	CHEQUE COPY RECEIPT.exe	Get hash	malicious	Browse	
	Remittance copy.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice 6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13166
Entropy (8bit):	3.774830690965141
Encrypted:	false
SSDEEP:	192:PnLf344LFHBUZMXaYuj7exr4/u7sBS274ItcmeN:fLf344L1BUZMXaYujX/u7sBX4ItcmeN
MD5:	B2A9FF4DD6892C2890DBF8E45AB88485
SHA1:	AE62CC1D9906E6551FA100EEFE60CA707B8D2091

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice 6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\Report.wer	
SHA-256:	E105583F6C4CA31C0D3884D7FE2F99C628F13B8595E78A0CF4690C2F3E830DB0
SHA-512:	508B06B0E8E9D8B5C8EF54867F11E19FD90A6C956CC14AEECC2C3533135190D28F9971F56433423564656A7018A0E02F84681FBF0E3BB87E66BB0B781334D386
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.4.9.4.7.9.8.5.7.4.7.1.7.7.....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.=.1.3.2.5.8.4.9.4.8.0.5.0.2.7.8.2.2.7.....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.=.0.6.3.8.7.8.1.4.-.d.b.5.2.-.4.f.b.a.-.8.7.9.f.-.f.3.f.1.c.0.3.c.2.c.9.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.b.a.c.3.8.0.6.-.2.e.b.4.-.4.3.3.f.-.a.3.b.3.-.5.4.4.b.4.9.1.6.8.5.7.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.n.v.o.i.c.e. .6.5.0.0.T.H.2.1.Y.5.6.7.4...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.8.c.-.0.0.0.1.-.0.0.1.b.-.b.4.9.d.-.c.2.c.4.4.e.0.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.7.b.7.9.2.2.d.7.e.0.b.6.4.7.f.5.2.4.4.9.5.7.e.4.8.1.5.b.1.5.e.0.0.0.0.0.9.0.4.!.0.0.0.0.6.5.d.3.e.4.f.4.d.f.3.4.b.b.2.5.f.7.b.6.2.1.d.d.0.4.5.7.c.6.4.1.f.9.8.0.2.9.c.b.!.I.n.v.o.i.c.e. .6.5.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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):	8344
Entropy (8bit):	3.703256214725214
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNifFH6IRrrGe6YrrSUgRtFgmfMuSj+pr/89bANsfTgm:RrlsNifl6IRrD6YnSUgRPgmfMuSHAGfx
MD5:	541615E3CF2661403307AEEE0CA852BC
SHA1:	E79D147C52E6A112639D2BB0A17B4165EAC69B2F
SHA-256:	63B424AD7CB406D35F481A902A4DBB8573096050392DF751B1C94A58BEEFE6D4
SHA-512:	FB921B062B06EE2EF18CDFCB57DD65F7A5C69C99EC92550C5D70EA8F03E018FF0C82BE20E994A2AF4AFC8498C6E4093F9A27EB6E8F4EEB91E0A62DCC420DA93A
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.>.7.0.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4623
Entropy (8bit):	4.48617925721146
Encrypted:	false
SSDEEP:	48:cvIwSD8zsSJgtWI9ajQWSC8BY8fm8M4JslB7qNuGFTiMo+q8Pn7623t2OXiveidd:uITfg9pSNzJk7dioe7192OSvJdd
MD5:	0B4DAE1146BC4C6A596446CEEBB2EDAB
SHA1:	D26B2B8C74DBE4B3853260F82AF6F7DA1915750D
SHA-256:	9FD8606D6D972D12DBB295F49C527C5C91DF75C38A190690CC8C1B4AEA5DAF78
SHA-512:	29AAEDB659300032FA468E4C67AD46FD1E2F8EB6D94D4FEAE10586F9BD966870F8DCA2D089A4B84E9B2D9158BE864386518C47AFC3E809FAD810697E98FDB4F
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="872904" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 22 19:13:21 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	66182
Entropy (8bit):	2.1500581148642697
Encrypted:	false
SSDEEP:	384:wSuP3ieR98ED6uAxxe3gzhZjr7hiEOGZn6K7:wSuPfR9LD6/xe3gzhZjr7hZ9n6Q
MD5:	C7B0D98301EDFA9EF17D07978828CED2
SHA1:	2A245600875BF190BF70026E71F4D23241572B86
SHA-256:	6C2C49E5548E9F64A1329C11717C88FBA8A904FE384A47FF7091E5456A019A29

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	
SHA-512:	C33DD77D9B22275C564E05A7AD6189C65C9C013E91142890CA441AF4052F69BD0A9C717A9322E5B2CF96ABE397989A1969D19F47C36A8A2E17149A9273F3FAC
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....Q.4`.....U.....B.....!.....GenuineIntelW.....T.....J.4`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\Users\user\AppData\Local\Temp\csnalztt.zl	
Process:	C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998912168321662**
Encrypted:	**true**
SSDEEP:	3072:vjvBirrhYZ6EhU+VR/zSRz3DInq5u+bFGLESasrlOqs621Ov4hrjlg:vjvBA+ESZBzSRz3DwNAHsr47x1Ov4h6
MD5:	56F7AC02D44E2C397DD1290AA89650A8
SHA1:	790FD108F1870FA972269CB1F8B2DEB71EB7CACA
SHA-256:	6A2E176536A074D8B73F52CA163CD414685662FF9372E964D075DA84E3F9A3EC
SHA-512:	5904B945CF35CB93CE6CE28608CC7A1689696DFD0AA217B153EBF3057C84B0F6B70B4AD4DBAC106D161C77B7E7B8A96B79175EBEFF2D1CB7AC119E92D0C0261
Malicious:	false
Reputation:	low
Preview:	fY.....i!3.J....H?T.)u...W..I-^Z.....>.....y>.*E.vh.|..YU..[iJ...@.'.'.....ba.u.0.1:.B)...^.3.5...N@*....o m@.....F.L."..&IB-.HnG<a.^...Xd..%.+.Z..E.X.s....[.?....j.....Dc.Y..I.....P.....EI.6.bf.$..<c.xkCC....,...I..'.bHm..H.D.1..q'....[..).7.K.A.....d.`.y.`.&.!.<S..2T..$v.Cp..Z.dk...Wo.....{.-V.....A.....;...p.....o.OG..92.{U.A.tf..&^.4.....#.3w.5.p.,.f..v4.h.*....%.oJ... t..."..BU..b.@!.d.Jw...].8o.,.<.{..B...I.\+C.A:I.....A.z<JVL....X...6..V.rj+n...fUYF....I-.7..`.....r..i...I.O..lz?.U....0..Sa..;nr..V...8G.....Yi0L...T..s.....L.O...tM9P.....Bm..j..".../=._0...+.\..P.....p.tt Y.S.w%Y..._i.X..+>Y&...y*..(.k...k.._....i...|./`.w..;..`~.,.....l?.....L.3.x.s.."....V..^L.....:>..A..)..."R..?..7...".kg$..o.t..{...G..(..R .....!.F.2..G...h...`..Z..gg.+..b3H..m...zz.OS....NP.8...;.;....m.fP..2.....~M...-..eP... 3R2d;[.T...U...N;(.....Q.y5t..n...M.`.?.....Z..2j.z..rQ*._..F.x....S.R.;.....f.#:#....DT

C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	
Process:	C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	6.36613341806139
Encrypted:	false
SSDEEP:	96:WkB+SnWJ9nZE0vhI2B3cubTsVoeMzr+o1s0klKGIvxzj13IDmZU7ukhMAzN+2:W4T0vhtlbDklKGM13y37ukhp+
MD5:	27352D6A2DA80C7A04C0A589E7F025BD
SHA1:	500B490B02EE59DEEE00FEB4C59A9F0308464E5C
SHA-256:	427AB077A32D2844F5E82A1D0C52B9FA73BB58298DC70B3D3A55BA05552DD840
SHA-512:	5AFC122644CA2D1B2F9594ADF653BE281001C6C4E4D6D31B55950B83C64A1434B63054594B575510A9FA707D33E22624F01E92F5DA2572712E364C7E1C21108B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 33%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../e..k.y.k.y.k.y..fx.`.y.k.x.y.y..Zq.j.y..Zy.j.y..Z{.j.y.Richk.y.....PE..L...`.`.....!..... .....P..... ` ..L.... ..x..... ..`.....tex t..... ..`.rdata..... .....@..@.data.....0.....@.....

C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	
Process:	C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C

C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: GPP.exe, Detection: malicious, Browse • Filename: OrderSuppliesQuote0817916.exe, Detection: malicious, Browse • Filename: ACCOUNT DETAILS.exe, Detection: malicious, Browse • Filename: Quotation.com.exe, Detection: malicious, Browse • Filename: Unterlagen PDF.exe, Detection: malicious, Browse • Filename: QuotationInvoices.exe, Detection: malicious, Browse • Filename: PO.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.24882.exe, Detection: malicious, Browse • Filename: PDF_doc.exe, Detection: malicious, Browse • Filename: 09000000000000.jar, Detection: malicious, Browse • Filename: quotation10204168.dox.xlsx, Detection: malicious, Browse • Filename: notice of arrivalpdf.exe, Detection: malicious, Browse • Filename: R5BNZ68i0f.exe, Detection: malicious, Browse • Filename: payment.exe, Detection: malicious, Browse • Filename: notice of arrival.xlsx, Detection: malicious, Browse • Filename: Invoice Overdue.exe, Detection: malicious, Browse • Filename: Invoice Overdue.exe, Detection: malicious, Browse • Filename: CHEQUE COPY RECEIPT.exe, Detection: malicious, Browse • Filename: Remittance copy.xlsx, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.888760018796244
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Invoice 6500TH21Y5674.exe
File size:	215032
MD5:	dc22d7783144cfe4dcbb4734ed6a3656
SHA1:	65d3e4f4df34bb25f7b621dd0457c641f98029cb
SHA256:	c9fc9a54366452a99c7ed753c7f5055141bc579b1a2530f8db7d7a039db6225d
SHA512:	908395a21d0a9411d8d2839b7c952f1cf50fd1998c5325457913cc27b581719d890919c196460ce5eb9fadba874b40043a537e8e40ff6aac75fd0dffcae7be4c
SSDEEP:	6144:7x/MzpANjvBA+ESZBzSRz3DwNAHsr47x1Ov4h9:RcpKjTyR7Dw347xkv4h9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.@.@...@...@../O...@...@..L@../O...@...c...@..+F...@..Rich.@.....PE..L...%.$_.....d....9.....%3.....@

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403325
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D625 [Sat Aug 1 02:40:37 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A2F6Ch], eax
je 00007F11E8839383h
push ebx
call 00007F11E883C4E6h
cmp eax, ebx
je 00007F11E8839379h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F11E883C462h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F11E883935Dh
push 0000000Bh
call 00007F11E883C4BAh
push 00000009h
call 00007F11E883C4B3h
push 00000007h
mov dword ptr [007A2F64h], eax
call 00007F11E883C4A7h
cmp eax, ebx
je 00007F11E8839381h
push 0000001Eh
call eax
test eax, eax
je 00007F11E8839379h
or byte ptr [007A2F6Fh], 00000040h
push ebp

Instruction
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [007A3038h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0079E528h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x988	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6230	0x6400	False	0.6699609375	data	6.44188995255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.4337890625	data	5.06106734837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x399078	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x988	0xa00	False	0.455859375	data	4.32856157213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x3ac148	0x100	data	English	United States
RT_DIALOG	0x3ac248	0x11c	data	English	United States
RT_DIALOG	0x3ac364	0x60	data	English	United States
RT_VERSION	0x3ac3c4	0x284	data	English	United States
RT_MANIFEST	0x3ac648	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

Description	Data
LegalCopyright	Copyright Abkhazian (Latin script)
FileVersion	8.96.29.2
CompanyName	decoration
LegalTrademarks	Hokkaido
Comments	Kalumpang
ProductName	fire escape
FileDescription	Liv
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

UDP Packets

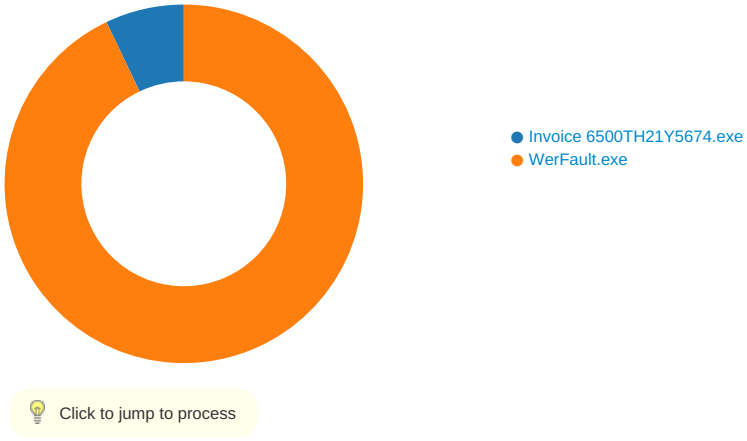
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:13:08.126100063 CET	65298	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:08.174998999 CET	53	65298	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:09.268579960 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:09.318689108 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:09.777106047 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:09.845844030 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:10.215289116 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:10.265507936 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:11.212158918 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:11.270188093 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:12.428859949 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:12.482754946 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:13.729577065 CET	49257	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:13:13.778476000 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:14.978543997 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:15.032226086 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:16.086262941 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:16.134982109 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:17.056094885 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:17.107492924 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:18.172137976 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:18.223676920 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:19.194848061 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:19.243395090 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:20.332845926 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:20.381582022 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:21.520343065 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:21.580420017 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:22.551676035 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:22.603544950 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:23.776237965 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:23.826596975 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:24.780412912 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:24.830338001 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:26.258446932 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:26.312314987 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:26.752038002 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:26.800841093 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:27.809377909 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:27.859285116 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:38.105026960 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:38.156537056 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:57.876569033 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:57.940486908 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:58.460304976 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:58.565757990 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:59.057368994 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:59.126800060 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 20:13:59.376662970 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:13:59.439727068 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:00.561758995 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:00.634332895 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:01.538045883 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:01.600204945 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:02.156744957 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:02.216437101 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:02.888663054 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:02.918108940 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:02.966742039 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:02.976929903 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:04.285130978 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:04.345084906 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:05.629309893 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:05.679775953 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:06.269172907 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:06.326704979 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:13.891426086 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:13.940160036 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:14.219197989 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:14.284236908 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:16.800393105 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:16.861208916 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:50.368153095 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:50.417006969 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 20:14:52.280946970 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:14:52.338311911 CET	53	49228	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Invoice 6500TH21Y5674.exe PID: 7052 Parent PID: 5920

General

Start time:	20:13:14
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe'
Imagebase:	0x400000
File size:	215032 bytes
MD5 hash:	DC22D7783144CFE4DCBB4734ED6A3656
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmED28.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\csnalztt.zl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\nshED58.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshED58.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40570A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmED28.tmp	success or wait	1	40359C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nshED58.tmp	success or wait	1	4058CB	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ir9ehshgyir.dll	unknown	8192	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2f 65 17 ca 6b 04 79 99 6b 04 79 99 6b 04 79 99 18 66 78 98 60 04 79 99 6b 04 78 99 79 04 79 99 de 5a 71 98 6a 04 79 99 de 5a 79 98 6a 04 79 99 de 5a 7b 98 6a 04 79 99 52 69 63 68 6b 04 79 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 05 60 2e 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 00 00 04 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......./e..k.y.k.y.k.y..fx.`. y.k.x.y.y..Zq.j.y..Zy.j.y..Z{. j.y.Richk.y.................PE ..L....`.`...........!........	success or wait	1	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\csnalztt.zl	unknown	32768	66 59 2e ea fa 8d 0f 88 0a e2 69 21 33 1d 4a de d3 e2 f2 48 3f 54 e6 29 75 8d 86 1b 57 92 03 6c 2d 5e 5a 0b 10 c5 c8 d2 9e 3e 97 f1 b6 d0 b4 a3 a4 fe a4 ce c5 79 3e e5 2a 45 d8 76 68 f4 7c ff 90 59 55 e0 0c 5b 69 4a 8b 17 db 40 e5 95 27 f5 27 a7 15 bd 8f 11 90 1a ee 62 61 1e 75 17 30 fb 31 3a cd 89 42 29 05 f1 e0 5e ef 97 33 e0 35 e0 f7 2e 4e 40 2a 14 a6 ba fd 6f 20 6d 40 e2 ab c0 88 1a 8a 46 f0 4c 05 22 82 c2 26 49 42 2d e2 48 6e 47 3c 61 b2 5e c4 00 ae 58 64 0a f5 25 a1 2b c9 5a 0d db 45 ca 58 e6 81 90 73 e5 d2 02 f6 5b e3 3f bc c2 ad e9 fb 6a 17 0d 1e c8 b1 c6 f8 44 63 8b 59 16 b9 6c 2e 8c 11 f8 af dc 0d af bc 91 50 ae a3 f6 b9 2e 45 49 be 36 e9 62 66 f9 24 c1 81 3c 63 07 78 6b 43 43 a6 ac b7 b4 2c 14 93 97 6c d4 09 27 e2 b7 62 48 6d da 96 9f 48 c0 44	fY........i!3.J....H?T.)u...W. .l-^Z......>...........y>.*E.v h.|..YU..[iJ...@..'.'........b a.u.0.1:..B)...^..3.5...N@*... .o m@......F.L."..&IB- .HnG<a.^ ...Xd..%.+.Z..E.X...s....[.?.. ...j.......Dc.Y..l..........P. ....El.6.bf.$..<c.xkCC....,... l..'..bHm...H.D	success or wait	6	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshED58.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405D2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe	unknown	512	success or wait	71	405CFF	ReadFile
C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\Desktop\Invoice 6500TH21Y5674.exe	unknown	4	success or wait	11	405CFF	ReadFile

Analysis Process: WerFault.exe PID: 1320 Parent PID: 7052

General

Start time:	20:13:16
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7052 -s 740
Imagebase:	0x60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6CF61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	success or wait	1	6CF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	success or wait	1	6CF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp.xml	success or wait	1	6CF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB20.tmp.csv	success or wait	1	6CF54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE0.tmp.txt	success or wait	1	6CF54BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 51 02 34 60 a4 05 12 00 00 00 00 00	MDMP..... .....Q.4`.....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.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 e8 21 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 8c 1b 00 00 4a 02 34 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B.......!.... ..GenuineIntelW...........T... ....J.4`.................. ....0..................W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 c4 6f 10 00 00 00 00 0c 00 00 00 40 5a b7 73 00 cb 86 04 00 cb 86 04 fc f1 19 00 fd 31 00 10 23 00 00 00 06 02 01 00 50 ea 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+......o........@Z.s........ .....1..#.......P...+.........	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	168	90 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 fd 31 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 cb 86 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 46 28 00 00	.........................1.... ....F(..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	20	1f 00 00 00 c4 fd cc 00 00 00 00 00 3c 02 00 00 ce 3d 00 00	............<....=..	success or wait	31	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	572	bc b1 11 77 d6 c9 0f 77 90 00 00 00 aa aa aa aa 10 00 00 00 58 fe cc 00 24 ff cc 00 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 90 23 00 00 90 23 00 00 00 00 00 90 00 00 00 aa aa aa aa 90 00 00 00 aa aa aa aa 00 90 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 4d 9d 00 00 00 00 00 00 00 00 00 e8 31 9d 00 00 00 23 00 10 00 00 00 aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 9d 02 90 fe bc 00 98 fe bd 02 98 fe bc 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w............X...$..... ..@..w@..w......#...#......... ....#............... ....M.... ....1....#................	success or wait	30	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	9644	bc 9a 11 77 a3 1a ae 74 aa aa aa aa 88 dc 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 e8 02 00 00 f4 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 88 dc 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...t...................... ....$........... .... #.............................	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	4	06 00 00 00	....	success or wait	6	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.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 40 5a b7 73 aa aa aa aa 00 00 00 00 e8 db 19 00 bc 9a 11 77 23 00 00 00 02 02 00 00 58 da 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+...............@Z.s........ ....w#.......X...+.........	success or wait	6	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	48	ac 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 24 00 00 00 00 00 c4 fd bd 02 00 00 00 00 3c 02 00 00 e6 a8 00 00 cc 02 00 00 0e 39 00 00	.... $............ <............9..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	4	37 00 00 00	7...	success or wait	55	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	56	32 00 00 00 49 00 6e 00 76 00 6f 00 69 00 63 00 65 00 20 00 36 00 35 00 30 00 30 00 54 00 48 00 32 00 31 00 59 00 35 00 36 00 37 00 34 00 2e 00 65 00 78 00 65 00 00 00	2...I.n.v.o.i.c.e. .6.5.0.0.T.H.2.1.Y.5.6.7.4...e.x.e...	success or wait	55	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	752	00 00 ec 6e 00 00 00 00 00 c0 00 00 1a 2f 01 00 25 80 23 fc 14 28 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d4 02 00 00 00 00 00 70 ff 02 00 00 00 00 df 4e 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 31 75 03 00 00 00 00 00 31 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 26 1b 00 00 00 00 00 12 d9 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 d5 f1 04 00 00 00 00	...n...../..%.#..(.....B.....B?...../.....@A.....Zb.....P.....p.....N.....1u.....1u.....&.....@.....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	11348	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB9F.tmp.dmp	unknown	108	03 00 00 00 24 01 00 00 fc 06 00 00 04 00 00 00 38 17 00 00 2c 08 00 00 05 00 00 00 f4 01 00 00 da 3b 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 d8 1e 00 00 f6 e3 00 00 15 00 00 00 ec 01 00 00 64 1f 00 00 16 00 00 00 98 00 00 00 50 21 00 00	....$.....8...,..... ...;.....T.....8..... ....T..... ..d.....P!..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.5.2.<./.P.i.d.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 49 00 6e 00 76 00 6f 00 69 00 63 00 65 00 20 00 36 00 35 00 30 00 30 00 54 00 48 00 32 00 31 00 59 00 35 00 36 00 37 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.I.n.v.o.i.c.e. .6.5.0.0.T.H.2.1.Y.5.6.7.4...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 33 00 38 00 37 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.>.7.3.8.7.<./.U.p.t.i.m.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 39 00 37 00 30 00 37 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.0.9.7.0.7.2.6.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 39 00 36 00 39 00 39 00 30 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.0.9.6.9.9.0.7.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 35 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.5.7.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 32 00 30 00 39 00 30 00 32 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.>.1.4.2.0.9.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 32 00 30 00 39 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.2.0.9.0.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 33 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.3.8.6.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 33 00 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.3.2.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 35 00 38 00 32 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.>.5.8.2.3.2.<./.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 35 00 37 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.7.9.6.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 33 00 35 00 31 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.3.5.1.0.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 34 00 33 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.4.3.2.9.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 33 00 35 00 31 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.9.3.5.1.0.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 31 00 31 00 32 00 38 00 35 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.1.1.2.8.5.2.<./.U.p.t.i.m.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 37 00 39 00 36 00 39 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.>.4.7.9.6.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 35 00 36 00 33 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.6.3.5.8.4.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 30 00 30 00 30 00 30 00 32 00 30 00 32 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.0.0.2.0.2.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 33 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.3.1.5.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 32 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.2.1.9.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 34 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.6.5.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 32 00 33 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.3.2.0.<./.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 30 00 35 00 38 00 34 00 38 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.5.8.4.8.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 31 00 35 00 34 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.>.3.8.1.5.4.2.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 30 00 35 00 38 00 34 00 38 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.5.8.4.8.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 49 00 6e 00 76 00 6f 00 69 00 63 00 65 00 20 00 36 00 35 00 30 00 30 00 54 00 48 00 32 00 31 00 59 00 35 00 36 00 37 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.I.n.v.o.i.c.e..6.5.0.0.T.H.2.1.Y.5.6.7.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 68 00 63 00 6e 00 71 00 6a 00 73 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.>.h.c.n.q.j.s.,. .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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 68 00 63 00 6e 00 71 00 6a 00 73 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.>.h.c.n.q.j.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 37 00 33 00 33 00 32 00 35 00 36 00 38 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.3.2.5.6.8.0.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 32 00 2d 00 32 00 32 00 54 00 31 00 39 00 3a 00 31 00 33 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.2.T.1.9.:.1.3.:.2.1.Z.".>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 35 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 37 00 34 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 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 34 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.0.". .P.I.D.=.".7.0.5.2.". .U.p.t.i.m.e.M.S.=.".7.4.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.4.9.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 36 00 33 00 38 00 37 00 38 00 31 00 34 00 2d 00 64 00 62 00 35 00 32 00 2d 00 34 00 66 00 62 00 61 00 2d 00 38 00 37 00 39 00 66 00 2d 00 66 00 33 00 66 00 31 00 63 00 30 00 33 00 63 00 32 00 63 00 39 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.6.3.8.7.8.1.4.-.d.b.5.2.-.4.f.b.a.-.8.7.9.f.-.f.3.f.1.c.0.3.c.2.c.9.f.<./.G.u.i.d.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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 32 00 2d 00 32 00 32 00 54 00 31 00 39 00 3a 00 31 00 33 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.2.T.1.9.:.1.3.:.2.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F4.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	6CF5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB12.tmp.xml	unknown	4623	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	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice 6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\Report.wer	unknown	2	ff fe	..	success or wait	1	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice 6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\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	185	6CF5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Invoice 6500TH21_a95a9cdbd3868a56584b72cabf593f6f9eaa3187_00d3adf0_05661bd9\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 33 00 34 00 34 00 37 00 39 00 31 00 34 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.0.3.4.4.7.9.1.4.8.	success or wait	1	6CF5497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	success or wait	1	6CF736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CF71FB2	RegCreateKeyExW
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	ProgramId	unicode	0006b7b7922d7e0b647f5244957e4815b15e00000904	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	FileId	unicode	000065d3e4f4df34bb25f7b621dd0457c641f98029cb	success or wait	1	6CF736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	LowerCaseLongPath	unicode	c:\users\user\desktop\invoice 6500th21y5674.exe	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	LongPathHash	unicode	invoice 6500th21|1c547b34	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	Name	unicode	invoice 6500th21y5674.exe	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	Publisher	unicode	decoration	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	Version	unicode	8.96.29.2	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	BinFileVersion	unicode	8.96.29.2	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	BinaryType	unicode	pe32_i386	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	ProductName	unicode	fire escape	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	ProductVersion	unicode		success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	LinkDate	unicode	08/01/2020 02:40:37	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	BinProductVersion	unicode	8.96.29.2	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	Size	B	F8 47 03 00 00 00 00 00	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	Language	dword	1033	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	IsPeFile	dword	1	success or wait	1	6CF736BF	unknown
\REGISTRY\A\{47b7cd9d-d8a7-e8a0-98b8-005fccced94e}\Root\InventoryApplicationFile\invoice 6500th21|1c547b34	IsOsComponent	dword	0	success or wait	1	6CF736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 FD 31 00 10 02 00 00 00 00 00 00 00 14 CB 86 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CF71FE8	RegSetValueExW

Disassembly

Code Analysis