ID: 349160
Sample Name: ioir.png.dll
Cookbook: default.jbs
Time: 15:10:14
Date: 05/02/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report ioir.png.dll

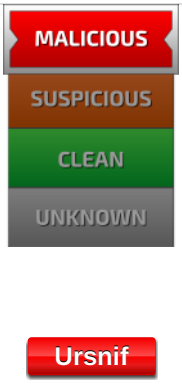
Overview

General Information

Sample Name:	ioir.png.dll
Analysis ID:	349160
MD5:	d31c0491f522d6b.
SHA1:	dc1cccf0e43ec5a..
SHA256:	f7c79c0c3feb7c0…
Tags:	isfbv3 ursnif

Most interesting Screenshot:

Detection

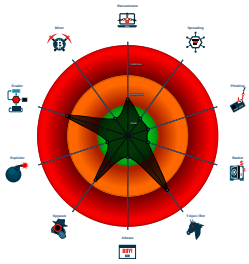


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Contains functionality to detect slee…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Checks if the current process is bein…
- Contains functionality for read data f…
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to check if a w…
- Contains functionality to detect sand…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6480 cmdline: loaddll32.exe 'C:\Users\user\Desktop\ioir.png.dll' MD5: 99D621E00EFC0B8F396F38D5555EB078)
  - rundll32.exe (PID: 3848 cmdline: rundll32.exe 'C:\Users\user\Desktop\ioir.png.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6308 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3848 -s 744 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- iexplore.exe (PID: 6588 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6748 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6588 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6952 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6588 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

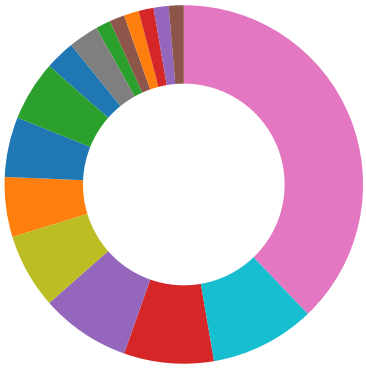
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.647244035.0000000005360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.648524337.0000000005360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.648667636.0000000005360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.648893530.0000000005360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.647868794.0000000005360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Stealing of Sensitive Information:

Yara detected Ursnif

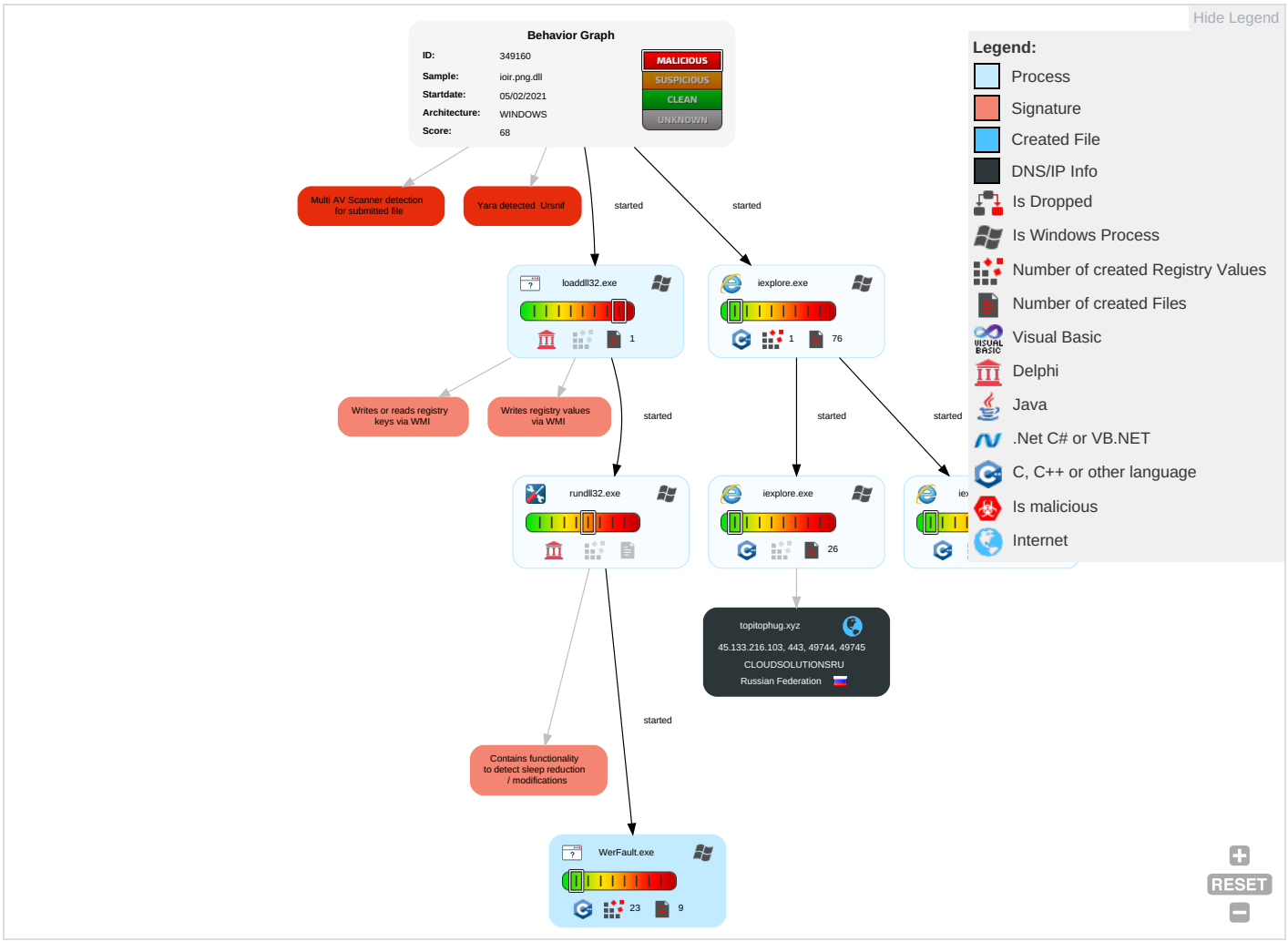
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 3	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

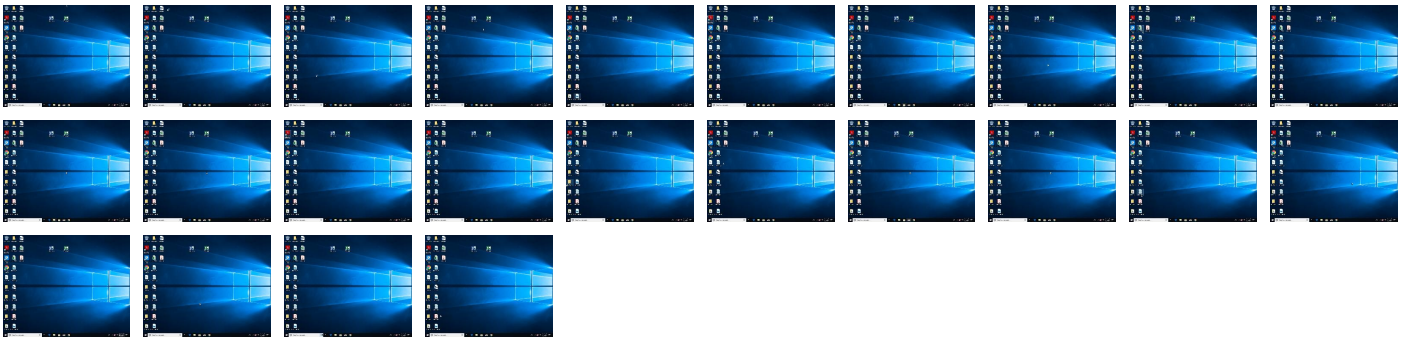
Behavior Graph



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
ioir.png.dll	42%	Virustotal		Browse
ioir.png.dll	41%	ReversingLabs	Win32.Trojan.Graftor	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.22d0174.3.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.2.loaddll32.exe.2790000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.rundll32.exe.3540000.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.rundll32.exe.3550000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
1.2.rundll32.exe.3530174.4.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.2.rundll32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
0.2.loaddll32.exe.2430000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://topitophug.xyz	0%	Avira URL Cloud	safe	
http://https://topitophug.xyz/index.htm/index.htm	0%	Avira URL Cloud	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://https://topitophug.xyz/index.htm	0%	Avira URL Cloud	safe	
http://https://topitophug.xyz/index.htmRoot	0%	Avira URL Cloud	safe	

Domains and IPs

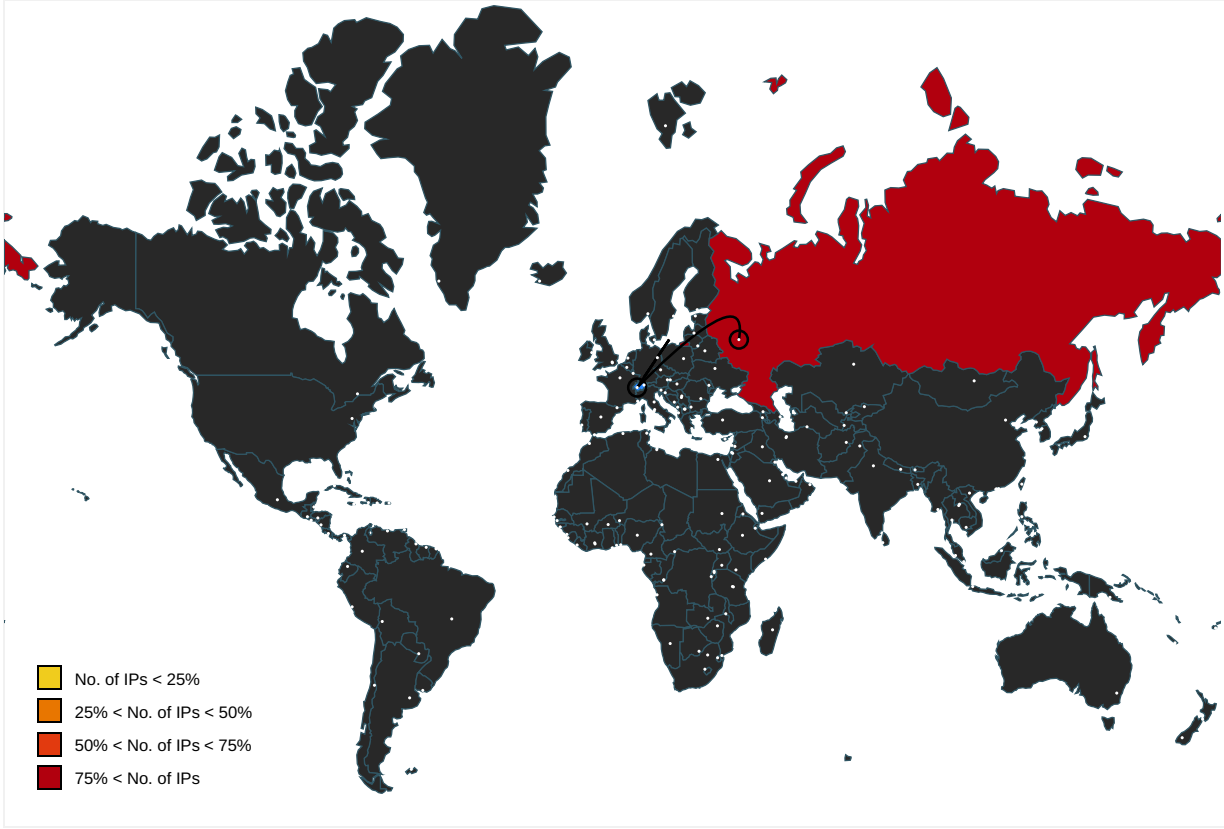
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
topitophug.xyz	45.133.216.103	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.8.dr	false		high
http://www.nytimes.com/	msapplication.xml3.8.dr	false		high
http://www.live.com/	msapplication.xml2.8.dr	false		high
http://https://topitophug.xyz	loaddll32.exe	false	• Avira URL Cloud: safe	unknown
http://https://topitophug.xyz/index.htm/index.htm	{FC8A972A-67BB-11EB-90EB-ECF4BBEA1588}.dat.8.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.8.dr	false		high
http://www.twitter.com/	msapplication.xml5.8.dr	false		high
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	loaddll32.exe, 00000000.00000003.648524337.0000000005360000.00000004.00000040.sdmp, rundll32.exe, 00000001.00000002.678292603.0000000008010000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://topitophug.xyz/index.htm	loaddll32.exe, 00000000.00000002.1020935253.0000000005360000.00000004.00000040.sdmp, ~DFF728301785477207.TMP.8.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.8.dr	false		high
http://https://topitophug.xyz/index.htmRoot	{FC8A972A-67BB-11EB-90EB-ECF4BBEA1588}.dat.8.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.133.216.103	unknown	Russian Federation		202933	CLOUDSOLUTIONSRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	349160
Start date:	05.02.2021
Start time:	15:10:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ioir.png.dll
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:	27
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:	mal68.troj.evad.winDLL@9/19@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 21.7% (good quality ratio 21.2%) • Quality average: 80.7% • Quality standard deviation: 22.7%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 88.221.62.148, 13.64.90.137, 51.104.139.180, 92.122.213.194, 92.122.213.247, 152.199.19.161, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:11:11	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDSOLUTIONSRU	facts-02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	facts-02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	facts-02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	decree.01.21.doc	Get hash	malicious	Browse	• 45.133.216.85

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	decree.01.21.doc	Get hash	malicious	Browse	• 45.133.216.85
	decree.01.21.doc	Get hash	malicious	Browse	• 45.133.216.85
	require 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	require 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	require 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	files 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	files 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	files 02.21.doc	Get hash	malicious	Browse	• 45.133.216.231
	statistics_02.01.2021.doc	Get hash	malicious	Browse	• 45.133.216.232
	statistics_02.01.2021.doc	Get hash	malicious	Browse	• 45.133.216.232
	statistics_02.01.2021.doc	Get hash	malicious	Browse	• 45.133.216.232
	document,01.21.doc	Get hash	malicious	Browse	• 45.133.216.55
	document,01.21.doc	Get hash	malicious	Browse	• 45.133.216.55
	document,01.21.doc	Get hash	malicious	Browse	• 45.133.216.55
	particulars_01.21.doc	Get hash	malicious	Browse	• 45.133.216.55
	enjoin-01.26.2021.doc	Get hash	malicious	Browse	• 45.133.216.55

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	umAuo1QklZ.dll	Get hash	malicious	Browse	• 45.133.216.103
	PO_2856_from_Giancarlo_Distributing_Inc.htm	Get hash	malicious	Browse	• 45.133.216.103
	B33383838558-857585.htm	Get hash	malicious	Browse	• 45.133.216.103
	#U260e#Ufe0fmsg0100February_report_2021.HTM	Get hash	malicious	Browse	• 45.133.216.103
	5aa085f0fa8592460e391052db9c94cd.exe	Get hash	malicious	Browse	• 45.133.216.103
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 45.133.216.103
	wys-02-03-21 Statement_763108aGF5ZGVuag==.htm	Get hash	malicious	Browse	• 45.133.216.103
	A6C8E866.xlsx	Get hash	malicious	Browse	• 45.133.216.103
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 45.133.216.103
	POrder.html	Get hash	malicious	Browse	• 45.133.216.103
	CONSTANTINE.xlsx	Get hash	malicious	Browse	• 45.133.216.103
	Document0098.html	Get hash	malicious	Browse	• 45.133.216.103
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 45.133.216.103
	d0b443110cf5a7bd05759c00fee8fdad.exe	Get hash	malicious	Browse	• 45.133.216.103
	univarusa-02-02-21 Statement_367096cmFuZHkuZnJpZWRsZXk=.htm	Get hash	malicious	Browse	• 45.133.216.103
	univarsolutions-01-02-21 Statement_607376Y2lhcmFuLmJyYW5pZmY=.htm	Get hash	malicious	Browse	• 45.133.216.103
	normaagu@herbalife.com.htm	Get hash	malicious	Browse	• 45.133.216.103
	CSWWOe1Gnx.html	Get hash	malicious	Browse	• 45.133.216.103
	ATROIGDFVX.htm	Get hash	malicious	Browse	• 45.133.216.103
	VM859-7757.htm	Get hash	malicious	Browse	• 45.133.216.103

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13306
Entropy (8bit):	3.7712108697295097
Encrypted:	false
SSDEEP:	192:Bdie0oX5aoHBUZMX4jed+GbfY/u7sXS274ItWcD:bioXEQBUZMX4jeQ/u7sXX4ItWcD
MD5:	463C84121A048AD2BA765E6FCB8865BC
SHA1:	0C05AC19A543BD8FFA7B1805665CE9355FCDA851
SHA-256:	EE13D7B66DC61E8A56A3BAD31BB9886CB23AB1FB397A373B0F71777A7922142C
SHA-512:	6C0684501DCACB2E3953AE3A54A8E819E4DFF9F9FDE6806D541CB4ACC4FAF3CB10716DE2C27B1D99F7E3D576A0A37D1705D7563BC56A4C9FF66F9C4BB075BC3

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\Report.wer	
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.=.1.3.2.5.7.0.0.7.8.6.5.4.6.6.8.5.2.9.....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.=.1.3.2.5.7.0.0.7.8.6.9.8.2.6.2.3.5.9.....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.=.3.b.0.2.9.2.f.5.-.e.4.b.a.-.4.8.6.e.-.b.f.e.0.-.2.4.f.e.2.1.a.f.0.2.4.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.d.f.5.7.f.9.f.-.7.3.6.a.-.4.5.c.0.-.b.9.2.0.-.c.b.0.0.d.c.8.7.1.2.2.0.....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.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.0.8.-.0.0.0.1.-.0.0.1.b.-.f.1.c.c.-.c.5.b.b.c.8.f.b.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Feb 5 14:11:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48792
Entropy (8bit):	2.1558382421313653
Encrypted:	false
SSDEEP:	192:iowXW8tpYtlAKw+OHRiMMC+n2V77O9T4teM9YaEsJI1iJnDmSBF:MXW8tpY7XdiMFb9w4teEYzsJVq8F
MD5:	D538781FC8355DF6F2667C82DE023F70
SHA1:	ED3A12ABADA87B9512C258D0BD73FA024E6B52E1
SHA-256:	13118910E6B24D2D3244B76EC5543912ADC6D7FA9BABC45C849516608E31994E
SHA-512:	8FBD9221B6BCD07BFE27E3304F89958027BE31C7B1E91C438608F4A4FD62BDBA04D77B2449EDA3B77240C479AFDE8937A743E92B339086E31F13BF10816D761
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....Q.`.....U.....B.....!.....GenuineIntelW.....T.....Q.`.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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):	8330
Entropy (8bit):	3.7035645163569257
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiaG6h6Ygd6cIMgmfTjSx+prw89b4b+sf5ejm:RrlsNir6h6Yq6ggmfTjS44b9f86
MD5:	B7DA6E395939A41BFE50A321C6D323DC
SHA1:	173E5842A3201431E9740B084F5DB43B30EDC59B
SHA-256:	68CBCC78BF4202BC2F6A4D1EB517525F6186F5EF5E6403640D9DDEB4B5348011
SHA-512:	F22C4A66A03EB697FE1B4A51A0F96EE1CDCE004BFAADB6C5285CEDAC0C4E435833FCD72F1F6293F30495E4BB9BB6928FA6284134A04E747500F02E27F966ACCA
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.>.3.8.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4669
Entropy (8bit):	4.500792046521803
Encrypted:	false
SSDEEP:	48:cvIwSD8zscJgtWI968WSC8B88fm8M4JCdsjZFT+q8/Oz44SrSkd:uITfa91SNvJ1/54DWkd
MD5:	513D059A55EF614427FDC28717F581FB
SHA1:	1A0F3336B77A7FF565C088BB040F5EE0C5674C6B
SHA-256:	DA3C44AD49F98340DBF30FE2FD22514889BC0144D7369F132EF3A3A073F3228F
SHA-512:	FB88AD7652000F59D2C891864E9F98525D7A9C99A199FE897467D5FCF83348E0E152FAB9A9374F0FEF06130E65A7B001B2AA876BDFFF0D01C0F3A4FBC33A4263
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp.xml	
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="848121" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FC8A9728-67BB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	41560
Entropy (8bit):	1.9329562369765705
Encrypted:	false
SSDEEP:	384:rFskBUzInE8/7E2DQeoBUoIEABmPP3Gem:fE8jE2DQpBHIfBSPWem
MD5:	59DFE51ACAC3DC82DE1F9E9FF0F1A687
SHA1:	E94CBCF03C7EE483A5ABF8006763E8E558C0EE74
SHA-256:	0A086E3BE77A657EFF1205D166F1659D38FA15A4390BBBAECCC6E77AF6D77F23
SHA-512:	EBE4D91785442F032E4A2EAF15F9FE9A0ED63DC7F5D049416FF702EA42CF9D8450C7A07ADA9F68C7CEBDB940DA80202654B52AF5FA476E3006626070DDC573E 9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4C399E10-67BC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5754992114408473
Encrypted:	false
SSDEEP:	48:IwdGcprUGwpaaG4pQO7GrapbS0xrGQpB9sGHHpcksTGUpG:rDZsQa6OvBSYFjJ2kkA
MD5:	9D4D9A4FF0756DA534B51497A1D1719B
SHA1:	74AE037703FEAEB0DB156F7256EDEBB0058E4109
SHA-256:	B89D970145E20B222A87A08B0CEC456D0308D5A0D74F8EB0B0FFCFB3A89571D6
SHA-512:	D4DA58D8A400ECC64D0CA61FA284B8C7D3C344279927C8D6F42B20A0838B473E385FA619FE21CA4F69E98808A1946D1E476F129C93AAE13A4FB2FAB951117C8
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC8A972A-67BB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26256
Entropy (8bit):	1.6642506081018853
Encrypted:	false
SSDEEP:	48:IwrGcprq7GwpaGG4pQuGrapbSKrGQpBKGHHpcRsTGUp83GzYpmLEYGop2JnOGiXD:rxZmQ26gBSKFjR2RkW1MYY8ilaRA
MD5:	7D46C19E4F6FB8B0F672D771F9DEBB3D
SHA1:	F1EA00C6ABB0C8A54D29FA6CD334B395DD780497
SHA-256:	35CE987AF57E0B56BE1D1EABDA3EDF343CEDDD15461AFD47E5B0B88C37BBCAE1
SHA-512:	C41B0DB9B9AA6B1520F7ADCE787DE17ED503BD273E4BC44C2151ADD92DC3A9F6674FDA6E30743918724DC8AEED2A1A261753C709D035FA23DE926B87A39B5 60
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.062751518107858
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEn1nWimI002EtM3MHdNMNxOEn1nWimI00OYGVbkEtMb:2d6NxOG1SZHKd6NxOG1SZ7YLb
MD5:	0CCC032CF24BAECD02966BFA35CFEC9A
SHA1:	D3DC1764ED72EEA6BBEC006A37C6391178AC4F9D
SHA-256:	CEC3931C2D9ABA751D0A659645012AA0EB397B6B68A1C1904A9D59037598B404
SHA-512:	B7488364AE0E6782F8D657717FD2BBFB6BC33902DA489A9C9A4630028BEE616F09E03E2359CBC4E823560361A676A05FCA4195928C4A91B8E53EE4E6428FAE1C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x19c13ca7,0x01d6fbc9</date><accdate>0x19c13ca7,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x19c13ca7,0x01d6fbc9</date><accdate>0x19c13ca7,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.118031973224068
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kYCXYDzCXYWnWimI002EtM3MHdNMNxe2kYCXYDzCXYWnWimI00OYGv:2d6NxrZDtWSZHKd6NxrZDtWSZ7Yza7b
MD5:	91823A87212DABC8ED12F03532097F23
SHA1:	E45CBC26A1C8F98D1734D1570EADEE978F96781A
SHA-256:	5081C81723D6ED587C4F09DB8A51E0C1DC773C3CF92E5AE340B9A8A0E5251A09
SHA-512:	D2A1BFB277428BA930269A15D0BE73D99A0E7F3A37CD6F52D5274B30998EF3198F6E48623C8AFC0E9F937E820CA4564DB9BC6CF6B24E9BE8585B85736C708B2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x19b7b33d,0x01d6fbc9</date><accdate>0x19b7b33d,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x19b7b33d,0x01d6fbc9</date><accdate>0x19b7b33d,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.084621789248435
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLn1nWimI002EtM3MHdNMNxvLnLU4nWimI00OYGmZEtMb:2d6Nxvj1SZHKd6NxvjTSZ7Yjb
MD5:	19E534F010FE9794ABAA6FD8A5D7821C
SHA1:	1CCC1A92A4636F9B06D0B28AC2CF2A7786BC6EB5
SHA-256:	4FC3DF159DC956A9DADB427E743EBFB4A3466FB616E0C47A74326757615A9424
SHA-512:	638DF1AC70867B83EC233B989790B6AD9F8B914696C53202DBF86A206FEBD00FE99AADACDBF5DA93B959907263C069DAFE26F6FDB9EBA0FFFD234228D46E489
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x19c13ca7,0x01d6fbc9</date><accdate>0x19c13ca7,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x19c13ca7,0x01d6fbc9</date><accdate>0x19c39f10,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.059389646415428

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxiYlXgzlXPnWimI002EtM3MHdNMNxiYlXgzlXPnWimI00OYGd5EtMb:2d6Nx8xSZHKd6Nx8xSZ7YEjb
MD5:	B6FA3DCE091C867063EF32063AE6B81A
SHA1:	D3195C1E01BB1972530342F0D52B9BCBAA6E7B2F
SHA-256:	DD68DE3424C37828039DADA7C67D4ECA2A8A3737CC0133B5B75E3D7555695B2A
SHA-512:	770ECC43E6AC205086D783C4D188CB18AA3DA1330FF7B8D5D3517B5F0F6D704DB95C0670D09982F366357F7C69C471863416B9AC20E00FF8F1398544EA430A7C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x19bedace,0x01d6fbc9</date><acc date>0x19bedace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x19bedace,0x01d6fbc9</date><accdate>0x19bed ace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msappl ication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.09564550749467
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwuURLU4nWimI002EtM3MHdNMNxhGwuURLU4nWimI00OYG8K075EtMb:2d6NxQETSZHKd6NxQETSZ7YrKajb
MD5:	9094C1234D482B9A1915A49405753F96
SHA1:	0C709B00AFD7AA6894765AFE0AF46DA00F5F3469
SHA-256:	6894497DA11891747996D117ABE91AE6B019DDDAC013B35922D10D81724143A1
SHA-512:	A9FB71A71B8F649D2684A74091FC1631EF6A463D9AEF74410009B8D1CABE8AF10A85499C63363F09200455ED31D47CA446D9B0CFA8497CCE88ECB224535C29C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x19c39f10,0x01d6fbc9</date>< accdate>0x19c39f10,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x19c39f10,0x01d6fbc9</date><accdate>0 x19c39f10,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.045598941850099
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nYlXgzlXPnWimI002EtM3MHdNMNx0nYlXgzlXPnWimI00OYGxEtMb:2d6Nx07xSZHKd6Nx07xSZ7Ygb
MD5:	01E3BA054B9DF29082673F4498AA3ACC
SHA1:	A9484E7746BB7DB069286B2E1016079E091C11D9
SHA-256:	6AE9E4CE2A51C5B2FB6A33D82BD12A2329F54131ECD6C139855E6B2E0A3CF394
SHA-512:	B98579B1140282268337 47A26AEA6D0CD129F5B99F49B1069DF737D8C68D10D917C44ECC0816ECA7A70CFF6C50EC14A419418E4946BB0108A07681A8AC2F728
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x19bedace,0x01d6fbc9</date><a ccdate>0x19bedace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x19bedace,0x01d6fbc9</date><accdate>0x1 9bedace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.084248903694253
Encrypted:	false
SSDEEP:	12:TMHdNMNxxYlXgzlXPnWimI002EtM3MHdNMNxxYlXgzlXPnWimI00OYG6Kq5EtMb:2d6NxRxSZHKd6NxRxSZ7Yhb
MD5:	B01C83D16D93DCF4CC58D190AAB45BB3
SHA1:	7472205652B35EE44052FD23EC5C329496D515D5
SHA-256:	AF1B635295959D24E3048A6043B73E9C591B8A6EA0F7B9CD0C82BBE55D731B67
SHA-512:	58B6C044FA1C54BC371CB6752324626B254EAF4D5A0379ECD27AB5C6EC7BC7C4487AD104F1104DA218BBDFEF6D1ECD3EAD062A8ACC14A79C82BB0DC9FAA2 F6B9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x19bedace,0x01d6fbc9</date><accdate>0x19bedace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x19bedace,0x01d6fbc9</date><accdate>0x19bedace,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.111048257686321
Encrypted:	false
SSDEEP:	12:TMHdNMNxcYob+Dzob+WnWimI002EtM3MHdNMNxcYob+Dzob+WnWimI00OYGVEtMb:2d6NxG+DS+WSZHKd6NxG+DS+WSZ7Ykb
MD5:	62FB4B45E2A3F029386C247BB8A2BA84
SHA1:	2D90B6B731A8D7F5D08B2E152955B202AC5C13E8
SHA-256:	207C81BAAB28B99E67D162EFCA4D25FEC95D75DED2D73C399E325F3B47E1BF68
SHA-512:	E443B7E77A6DA96944AC1235F3FB5D3907163258BBC56C25287EF1E3ACE5A759560FF9638362F5D2A846F00FF0C9CE7FA80F0C5C4FFB4D81F3E75A9F954BF1C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x19bc77f4,0x01d6fbc9</date><accdate>0x19bc77f4,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x19bc77f4,0x01d6fbc9</date><accdate>0x19bc77f4,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.100493240268499
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnYob+Dzob+WnWimI002EtM3MHdNMNxfnYob+Dzob+WnWimI00OYGe5t:2d6NxZ+DS+WSZHKd6NxZ+DS+WSZ7YLjb
MD5:	096B29C7136E02A5D60FDB8C68E4FCD8
SHA1:	B2E0EECDFC77383B8EBF414EC8EE9505B5D2CFD4
SHA-256:	EB5DC9F9660BECE895A734CDE556A1F300193F3C12D88FE59E5E1B67DA85B902
SHA-512:	4280346D4A6C326A34C456CB6ECE4FB6CFD98B6DA6E9F048ECB0C6B152B5FB40CD359A42B4146C42DD067CB9040BFAD04CF6158FBC1DDB1834FA6329D8951EE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x19bc77f4,0x01d6fbc9</date><accdate>0x19bc77f4,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x19bc77f4,0x01d6fbc9</date><accdate>0x19bc77f4,0x01d6fbc9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DFD3E7BA36C3F7FAA9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13061
Entropy (8bit):	0.4896474116676091
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loT9loT9lW8J+9ndGn:kBqoIUK8odGn
MD5:	95F888571CBFF9AB4950C0CE17A96C51
SHA1:	C78811B36C3C587978ABCE82849C01B3BA4E035E
SHA-256:	1AA2855877AFCDB15C440ED93AA9F6D222BD012EE47DE695D6E1470D588D8408
SHA-512:	FAEB37A77D46F91F1A81841D44E493D909C1115DFFF6C8ACD27BA3A4DDE62D199528DE13567C26CAC18B435B4597C488E9D5789E1A9AECEC36A8CE327AD43C4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE7AA1257DA4DC091.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DFE7AA1257DA4DC091.TMP	
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31361137561153196
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw9X9lw9Q69l29jy:kBqoxKAuvScS+yU4
MD5:	8D816B7B983F961ED3B9B509F017ED35
SHA1:	47A27C40157765E957C7E28139AF670C88F3BBDD
SHA-256:	50DB79CA883007EF294A69CC8D8E25B3DA50B81AFCD2F48531A3C0A2BF8E601F
SHA-512:	614FE9933ADDE0CAFC6891729C2934A9184468E66210CBEEB640E517B3FC92D73E8A607A27B91FB45A8053F6DB7D29E3676163BFA856D2841DA6BD15B137A4A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF728301785477207.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38753
Entropy (8bit):	0.37411054473392363
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwR9lwx9l2v9l2v9l/LK:kBqoxKAuvScS+CkuHLILIJnHJndJnu
MD5:	7AF44FCAD565F54FD92AD64011D18442
SHA1:	8A1946FA2C4C286A6E25F63308DEF800CBC48041
SHA-256:	563E1D0C449298884934CD1CD244848E193C0FC36A549FE29B8C9E05C922E507
SHA-512:	D3587D34852E34A8501B485B7FE5541C842E2F10580ED02573A44303531CC18A16332F3B7FE60CFBAC55288B505B612C7AFAD7D9BDC5B46F5BE9FFE289C4BE7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.763543992410411
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 97.97% • Win32 Executable Delphi generic (14689/80) 1.44% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	ioir.png.dll
File size:	552448
MD5:	d31c0491f522d6b9f2102109bd2420af
SHA1:	dc1cccf0e43ec5a68326ae4faf1a8cbc5ac00708
SHA256:	f7c79c0c3feb7c0032424f5f6a9bcdf78d1815ee53f807cc192c2c1f8f21270f
SHA512:	48d659660654800da4eb3909a06572dfcf5f05ebdfb8629fafdfeab601673e3377d9a3a241f4bd36c3f4f912ac838dbc73926f734bfa8a76ec43fa726b28c3bd
SSDEEP:	12288:XCY7z0vLfhyqJ0UYek/zLOmyK8rkApSc1jJFX:SWz09yqJ5Ye6PHuNScBJF
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General	
Entrypoint:	0x46980c
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	127ef7eee4def6f47e8e66d53f8ddc7c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFC4h
mov eax, 0046960Ch
call 00007FBA84DDB765h
xor ecx, ecx
mov dl, 01h
mov eax, dword ptr [00468FFCh]
call 00007FBA84E10F9Bh
mov dword ptr [0046CC30h], eax
mov eax, dword ptr [0046CC30h]
call 00007FBA84E152E4h
call 00007FBA84DD97E3h
mov eax, eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6d000	0x23e4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x13000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	0x7610	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x68840	0x68a00	False	0.523362828554	data	6.51070065198	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x6a000	0x12d4	0x1400	False	0.433984375	data	4.02181905914	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x6c000	0xc35	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x6d000	0x23e4	0x2400	False	0.369357638889	data	5.03762629251	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x70000	0x7610	0x7800	False	0.58466796875	data	6.61973320617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x13000	0x13000	False	0.732010690789	data	7.14558558427	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
F1	0x78b68	0xd204	data	English	United States
RT_CURSOR	0x85d6c	0x134	data		
RT_CURSOR	0x85ea0	0x134	data		
RT_CURSOR	0x85fd4	0x134	data		
RT_CURSOR	0x86108	0x134	data		
RT_CURSOR	0x8623c	0x134	data		
RT_CURSOR	0x86370	0x134	data		
RT_CURSOR	0x864a4	0x134	data		
RT_BITMAP	0x865d8	0x1d0	data		
RT_BITMAP	0x867a8	0x1e4	data		
RT_BITMAP	0x8698c	0x1d0	data		
RT_BITMAP	0x86b5c	0x1d0	data		
RT_BITMAP	0x86d2c	0x1d0	data		
RT_BITMAP	0x86efc	0x1d0	data		
RT_BITMAP	0x870cc	0x1d0	data		
RT_BITMAP	0x8729c	0x1d0	data		
RT_BITMAP	0x8746c	0x1d0	data		
RT_BITMAP	0x8763c	0x1d0	data		
RT_BITMAP	0x8780c	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0x878f4	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 49, next used block 48059	Russian	Russia
RT_DIALOG	0x87bdc	0x52	data		
RT_STRING	0x87c30	0x224	data		
RT_STRING	0x87e54	0x1ec	data		
RT_STRING	0x88040	0xec	data		
RT_STRING	0x8812c	0x39c	data		
RT_STRING	0x884c8	0xec	Hitachi SH big-endian COFF object file, not stripped, 17664 sections, symbol offset=0x65007200, 83907328 symbols, optional header size 28672		
RT_STRING	0x885b4	0xf8	data		
RT_STRING	0x886ac	0x1a8	data		
RT_STRING	0x88854	0x398	data		
RT_STRING	0x88bec	0x3e0	data		
RT_STRING	0x88fcc	0x3a8	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x89374	0x418	data		
RT_STRING	0x8978c	0x234	data		
RT_STRING	0x899c0	0xec	data		
RT_STRING	0x89aac	0x1b4	data		
RT_STRING	0x89c60	0x3e4	data		
RT_STRING	0x8a044	0x358	data		
RT_STRING	0x8a39c	0x2b4	data		
RT_RCDATA	0x8a650	0x10	data		
RT_RCDATA	0x8a660	0x288	data		
RT_RCDATA	0x8a8e8	0x443	Delphi compiled form 'TForm1'		
RT_RCDATA	0x8ad2c	0xed	Delphi compiled form 'TForm2'		
RT_GROUP_CURSOR	0x8ae1c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae30	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae44	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae58	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae6c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae80	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x8ae94	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x8aea8	0x14	data	Russian	Russia

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, TlsFree, TlsAlloc, LocalFree, LocalAlloc
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, StartPage, StartDocA, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtTextOutA, ExtCreatePen, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CharUpperW, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
kernel32.dll	MulDiv

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 84

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:11:09.010075092 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.010190010 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.075484037 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.075531006 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.075582981 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.075659990 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.082328081 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.083014965 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.147501945 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.147896051 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.150233984 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.150275946 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.150302887 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.150317907 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.150355101 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.150366068 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.152689934 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.152740002 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.152777910 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.152812004 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.152846098 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.152849913 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.181955099 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.182029009 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.247997999 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.248059034 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:11:09.248152971 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.248842955 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.248872042 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.248944998 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:11:09.314248085 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:12:09.146543026 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:12:09.146572113 CET	443	49744	45.133.216.103	192.168.2.4
Feb 5, 2021 15:12:09.146727085 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:12:09.146775007 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:09.593648911 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:09.593756914 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:09.880130053 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:09.880187988 CET	49744	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:09.880901098 CET	49745	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:09.991070032 CET	443	49745	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:21.885030985 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:21.954657078 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:21.955271959 CET	49777	443	192.168.2.4	45.133.216.103

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:13:21.959441900 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.024964094 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:22.027736902 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:22.027772903 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:22.027786970 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:22.027903080 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.044152975 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.109941959 CET	443	49777	45.133.216.103	192.168.2.4
Feb 5, 2021 15:13:22.110074997 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.111372948 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.111480951 CET	49777	443	192.168.2.4	45.133.216.103
Feb 5, 2021 15:13:22.176907063 CET	443	49777	45.133.216.103	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:10:57.127938032 CET	63153	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:10:57.177488089 CET	53	63153	8.8.8.8	192.168.2.4
Feb 5, 2021 15:10:58.288995981 CET	52991	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:10:58.335963964 CET	53	52991	8.8.8.8	192.168.2.4
Feb 5, 2021 15:10:59.215821028 CET	53700	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:10:59.265412092 CET	53	53700	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:00.274355888 CET	51726	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:00.330168009 CET	53	51726	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:02.153189898 CET	56794	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:02.200150013 CET	53	56794	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:03.184634924 CET	56534	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:03.242126942 CET	53	56534	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:04.454282999 CET	56627	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:04.500952005 CET	53	56627	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:05.451766014 CET	56621	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:05.498395920 CET	53	56621	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:07.445197105 CET	63116	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:07.492767096 CET	53	63116	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:07.784857988 CET	64078	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:07.845151901 CET	53	64078	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:08.941991091 CET	64801	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:08.999475002 CET	53	64801	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:09.272541046 CET	61721	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:09.321039915 CET	53	61721	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:10.246723890 CET	51255	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:10.293646097 CET	53	51255	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:11.079930067 CET	61522	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:11.127470970 CET	53	61522	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:11.267817020 CET	52337	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:11.314388037 CET	53	52337	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:12.454510927 CET	55046	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:12.505116940 CET	53	55046	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:13.434499979 CET	49612	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:13.481628895 CET	53	49612	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:14.607250929 CET	49285	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:14.656871080 CET	53	49285	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:21.144412041 CET	50601	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:21.196465015 CET	53	50601	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:25.537904978 CET	60875	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:25.596429110 CET	53	60875	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:37.780924082 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:37.830451965 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:38.495282888 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:38.543936014 CET	53	59172	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:38.787137032 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:38.840082884 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:39.506083012 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:39.554653883 CET	53	59172	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:11:39.807240009 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:39.867321968 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:40.026734114 CET	62420	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:40.081789970 CET	53	62420	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:40.521188021 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:40.570120096 CET	53	59172	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:40.660974026 CET	60579	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:40.715950012 CET	53	60579	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:40.862476110 CET	50183	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:40.931441069 CET	53	50183	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:41.526072025 CET	61531	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:41.575651884 CET	53	61531	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:41.802392960 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:41.851960897 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:42.033946991 CET	49228	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:42.083383083 CET	53	49228	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:42.521174908 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:42.567806959 CET	53	59172	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:42.717406988 CET	59794	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:42.772543907 CET	53	59794	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:43.363240004 CET	55916	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:43.418147087 CET	53	55916	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:44.343419075 CET	52752	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:44.398530960 CET	53	52752	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:45.485378027 CET	60542	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:45.540724993 CET	53	60542	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:45.818109035 CET	56448	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:45.867546082 CET	53	56448	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:46.537005901 CET	59172	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:46.577455997 CET	60689	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:46.583584070 CET	53	59172	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:46.625001907 CET	53	60689	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:47.379790068 CET	64206	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:47.437128067 CET	53	64206	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:56.759221077 CET	50904	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:56.808696985 CET	53	50904	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:57.357604027 CET	57525	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:11:57.406884909 CET	53	57525	8.8.8.8	192.168.2.4
Feb 5, 2021 15:11:59.997220993 CET	53814	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:12:00.055185080 CET	53	53814	8.8.8.8	192.168.2.4
Feb 5, 2021 15:12:31.420690060 CET	53418	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:12:31.467262983 CET	53	53418	8.8.8.8	192.168.2.4
Feb 5, 2021 15:12:33.305716038 CET	62833	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:12:33.354562998 CET	53	62833	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:21.816430092 CET	59260	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:21.874515057 CET	53	59260	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:51.537769079 CET	49944	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:51.597984076 CET	53	49944	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:52.531815052 CET	49944	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:52.583115101 CET	53	49944	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:53.532160997 CET	49944	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:53.582953930 CET	53	49944	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:55.547427893 CET	49944	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:55.607625961 CET	53	49944	8.8.8.8	192.168.2.4
Feb 5, 2021 15:13:59.563509941 CET	49944	53	192.168.2.4	8.8.8.8
Feb 5, 2021 15:13:59.612879992 CET	53	49944	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 15:11:08.941991091 CET	192.168.2.4	8.8.8.8	0xd178	Standard query (0)	topitophug.xyz	A (IP address)	IN (0x0001)
Feb 5, 2021 15:13:21.816430092 CET	192.168.2.4	8.8.8.8	0xf9eb	Standard query (0)	topitophug.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 15:11:08.999475002 CET	8.8.8.8	192.168.2.4	0xd178	No error (0)	topitophug.xyz		45.133.216.103	A (IP address)	IN (0x0001)
Feb 5, 2021 15:13:21.874515057 CET	8.8.8.8	192.168.2.4	0xf9eb	No error (0)	topitophug.xyz		45.133.216.103	A (IP address)	IN (0x0001)

HTTPS Packets

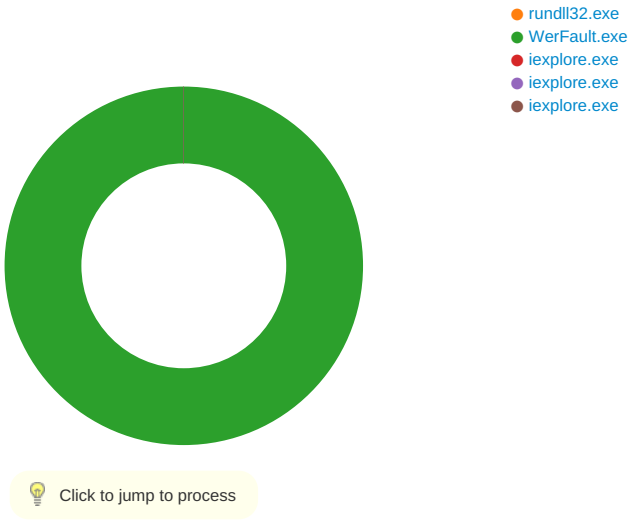
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 15:11:09.150275946 CET	45.133.216.103	443	192.168.2.4	49744	CN=topitophug.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 18 18:06:29 CET 2021	Sun Apr 18 19:06:29 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 5, 2021 15:11:09.152740002 CET	45.133.216.103	443	192.168.2.4	49745	CN=topitophug.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 18 18:06:29 CET 2021	Sun Apr 18 19:06:29 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 5, 2021 15:13:22.027772903 CET	45.133.216.103	443	192.168.2.4	49777	CN=topitophug.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 18 18:06:29 CET 2021	Sun Apr 18 19:06:29 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

● loaddll32.exe



System Behavior

Analysis Process: loaddll32.exe PID: 6480 Parent PID: 5884

General

Start time:	15:11:01
Start date:	05/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\ioir.png.dll'
Imagebase:	0x90000
File size:	121856 bytes
MD5 hash:	99D621E00EFC0B8F396F38D5555EB078
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647244035.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648524337.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648667636.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648893530.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647868794.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648751901.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648917284.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648176949.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648860307.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647426858.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647623145.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.649011597.0000000005360000.00000004.00000040.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647521163.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.649003327.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647703250.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.1020935253.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648956787.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648265573.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648974202.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647795143.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647330409.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.647948135.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648938200.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648374581.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648323443.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648615088.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648037894.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648828511.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648478035.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648792520.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648104820.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648425491.0000000005360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.648990980.0000000005360000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3848 Parent PID: 6480

General

Start time:	15:11:01
Start date:	05/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ioir.png.dll',#1
Imagebase:	0xde0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.678292603.0000000008010000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 6308 Parent PID: 3848

General

Start time:	15:11:03
Start date:	05/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3848 -s 744
Imagebase:	0x11a0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D2D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D2C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	success or wait	1	6D2C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	success or wait	1	6D2C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp.xml	success or wait	1	6D2C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD39.tmp.csv	success or wait	1	6D2C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEA.tmp.txt	success or wait	1	6D2C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 fb 51 1d 60 a4 05 12 00 00 00 00 00	MDMP..... .....Q.`.....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 c4 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 08 0f 00 00 f5 51 1d 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 31 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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... .....Q.`..... .....0..1.....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	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.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 04 3c 24 03 00 00 55 03 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 60 fa f0 02 b8 ca 53 03 23 00 00 00 93 02 01 00 5c fa f0 02 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...+...+.... <$...U................. \`.....S.#.......\...+.........	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	168	68 0b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 b8 ca 53 03 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 06 28 00 00	h.........................S... ....(..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	20	0e 00 00 00 c0 09 25 03 00 00 00 00 04 00 00 00 1a 34 00 00	......%..........4..	success or wait	14	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	4	c4 f9 4e 03	..N.	success or wait	13	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	4	14 12 0b 77	...w	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 f0 eb f0 02 bc 9a 11 77 23 00 00 00 16 02 00 00 60 ea f0 02 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	?............................ ....+...S...+. ..+.......................... ....w#.......`...+.........	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	48	d8 01 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 d0 1c 03 00 00 00 00 f8 f8 4e 03 00 00 00 00 08 07 00 00 c2 4b 00 00 cc 02 00 00 6a 30 00 00	....N... ....K......j0..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	4	38 00 00 00	8...	success or wait	56	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	56	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	752	00 00 ec 76 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 f2 27 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 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 20 c8 02 00 00 00 00 00 30 32 03 00 00 00 00 06 59 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 ac 73 03 00 00 00 00 00 2b 7a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7b 06 1b 00 00 00 00 00 c5 f8 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 ff fe 04 00 00 00 00	...v.....p.....(c>5.'..... .....B.....B?..... ....@E.....Zb..... ....02..... .Y.....s.....+z .....{..... @.....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	11354	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3C4.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 a4 17 00 00 9c 07 00 00 05 00 00 00 e4 00 00 00 36 33 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 28 1f 00 00 b8 9f 00 00 15 00 00 00 ec 01 00 00 40 1f 00 00 16 00 00 00 98 00 00 00 2c 21 00 00	....63.....T.....8..... ....T.....(..... ..@.....,!..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 38 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.8.4.8.<./.P.i.d.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.6.4.5.<./.U.p.t.i.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 38 00 31 00 35 00 38 00 37 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.8.1.5.8.7.9.6.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 37 00 34 00 39 00 36 00 38 00 38 00 33 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.>.1.7.4.9.6.8.8.3.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 36 00 31 00 38 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.>.3.6.1.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 32 00 37 00 34 00 36 00 37 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.2.7.4.6.7.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 31 00 32 00 34 00 33 00 35 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.1.2.4.3.5.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 34 00 34 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.4.4.5.4.4.<./.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 33 00 34 00 31 00 32 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.>.2.3.4.1.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 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.>.3.5.2.3.2.<./.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 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.>.3.4.9.6.0.<./.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 34 00 34 00 30 00 32 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.5.4.4.0.2.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 31 00 31 00 39 00 36 00 31 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.>.2.7.1.1.9.6.1.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 34 00 34 00 30 00 32 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.5.4.4.0.2.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.4.8.0.<./.P.i.d.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 39 00 34 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.>.5.9.9.4.<./.U.p.t.i.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 39 00 32 00 34 00 34 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.5.9.2.4.4.2.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 34 00 35 00 35 00 38 00 34 00 31 00 32 00 38 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.>.1.4.5.5.8.4.1.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 35 00 33 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.>.1.1.5.3.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 32 00 37 00 33 00 38 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.7.3.8.5.8.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 32 00 37 00 39 00 31 00 38 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.2.7.9.1.8.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 35 00 32 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.5.2.7.4.4.<./.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 35 00 38 00 38 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.>.2.2.5.8.8.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.5.0.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.3.0.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 37 00 39 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.2.7.9.1.6.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 30 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.9.0.8.3.5.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 37 00 39 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.2.7.9.1.6.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 72 00 78 00 71 00 77 00 76 00 79 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.r.x.q.w.v.y.,. .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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 78 00 71 00 77 00 76 00 79 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.r.x.q.w.v.y.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 33 00 30 00 34 00 35 00 37 00 37 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.3.0.4.5.7.7.0.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 30 00 35 00 54 00 31 00 34 00 3a 00 31 00 31 00 3a 00 30 00 37 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.-.0.5.T.1.4.:.1.1.:.0.7.Z.".>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 35 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 38 00 34 00 38 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 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 33 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.7.". .P.I.D.=.".3.8.4.8.". .U.p.t.i.m.e.M.S.=.".7.3.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.3.4.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 62 00 30 00 32 00 39 00 32 00 66 00 35 00 2d 00 65 00 34 00 62 00 61 00 2d 00 34 00 38 00 36 00 65 00 2d 00 62 00 66 00 65 00 30 00 2d 00 32 00 34 00 66 00 65 00 32 00 31 00 61 00 66 00 30 00 32 00 34 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.3.b.0.2.9.2.f.5.-.e.4.b.a.-.4.8.6.e.-.b.f.e.0.-.2.4.f.e.2.1.a.f.0.2.4.2.<./.G.u.i.d.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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 30 00 35 00 54 00 31 00 34 00 3a 00 31 00 31 00 3a 00 30 00 37 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.-.0.5.T.1.4.:.1.1.:.0.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA9B.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	6D2C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD2C.tmp.xml	unknown	4669	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	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\Report.wer	unknown	2	ff fe	..	success or wait	1	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\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	187	6D2C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_db99bffafeba5bc19edb8917aba4cdaba066d_82810a17_18f30ba1\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 39 00 34 00 34 00 30 00 37 00 34 00 30 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.3.9.4.4.0.7.4.0.8.	success or wait	1	6D2C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D2E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D2E1FB2	RegCreateKeyExW
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D2E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D2E36BF	unknown
\REGISTRY\A\{3b15354b-0de4-75e9-93a0-bf347b6f6b3d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D2E36BF	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 B8 CA 53 03 02 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 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	6D2E1FE8	RegSetValueExW

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

Analysis Process: iexplore.exe PID: 6588 Parent PID: 800

General

Start time:	15:11:06
Start date:	05/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f1c20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6748 Parent PID: 6588

General

Start time:	15:11:07
Start date:	05/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6588 CREDAT:17410 /prefetch:2
Imagebase:	0x10e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6952 Parent PID: 6588

General

Start time:	15:13:20
Start date:	05/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6588 CREDAT:17418 /prefetch:2
Imagebase:	0x10e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis