ID: 392878
Sample Name: gsG7jGFk3l
Cookbook: default.jbs
Time: 23:32:00
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

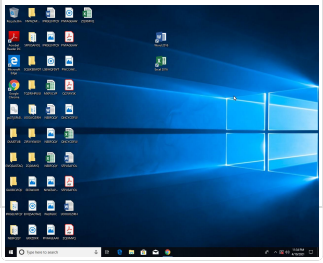
Analysis Report gsG7jGFk3l

Overview

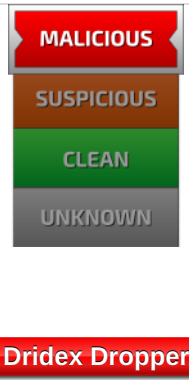
General Information

Sample Name:	gsG7jGFk3l (renamed file extension from none to dll)
Analysis ID:	392878
MD5:	e8675c9ab1bb95..
SHA1:	c088263ed0a68c..
SHA256:	6934bf4b117408d.
Tags:	40111 Dridex
Infos:	

Most interesting Screenshot:



Detection



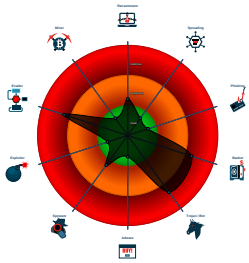
Dridex Dropper

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

Signatures

- Dridex dropper found
- Found malware configuration
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to delay execution (extensive O…
- Tries to detect sandboxes / dynamic…
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to query locale…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 1712 cmdline: loaddll32.exe 'C:\Users\user\Desktop\gsG7jGFk3l.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 668 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3l.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4832 cmdline: rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3l.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4516 cmdline: rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3l.dll',ReadLogRecord MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 4480 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1712 -s 428 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 40111,
  "C2 list": [
    "94.247.168.64:443",
    "159.203.93.122:8172",
    "50.116.27.97:2303"
  ],
  "RC4 keys": [
    "VOw9c7u110XYjoFF2SzRWNcWNob7Sec1HxEVgBrFF",
    "5gZeCc8o5cQELWnF44Ik184W6MoZ25O98Rol7kPT2itFWvdxWiT70K4o4YnFUN4mL"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.495709984.000000006E881000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.494850916.000000006E881000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

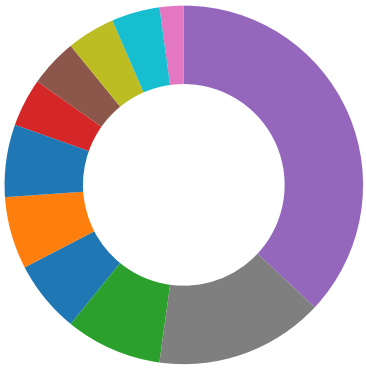
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.6e880000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.6e880000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Dridex dropper found

Yara detected Dridex unpacked file

Malware Analysis System Evasion:

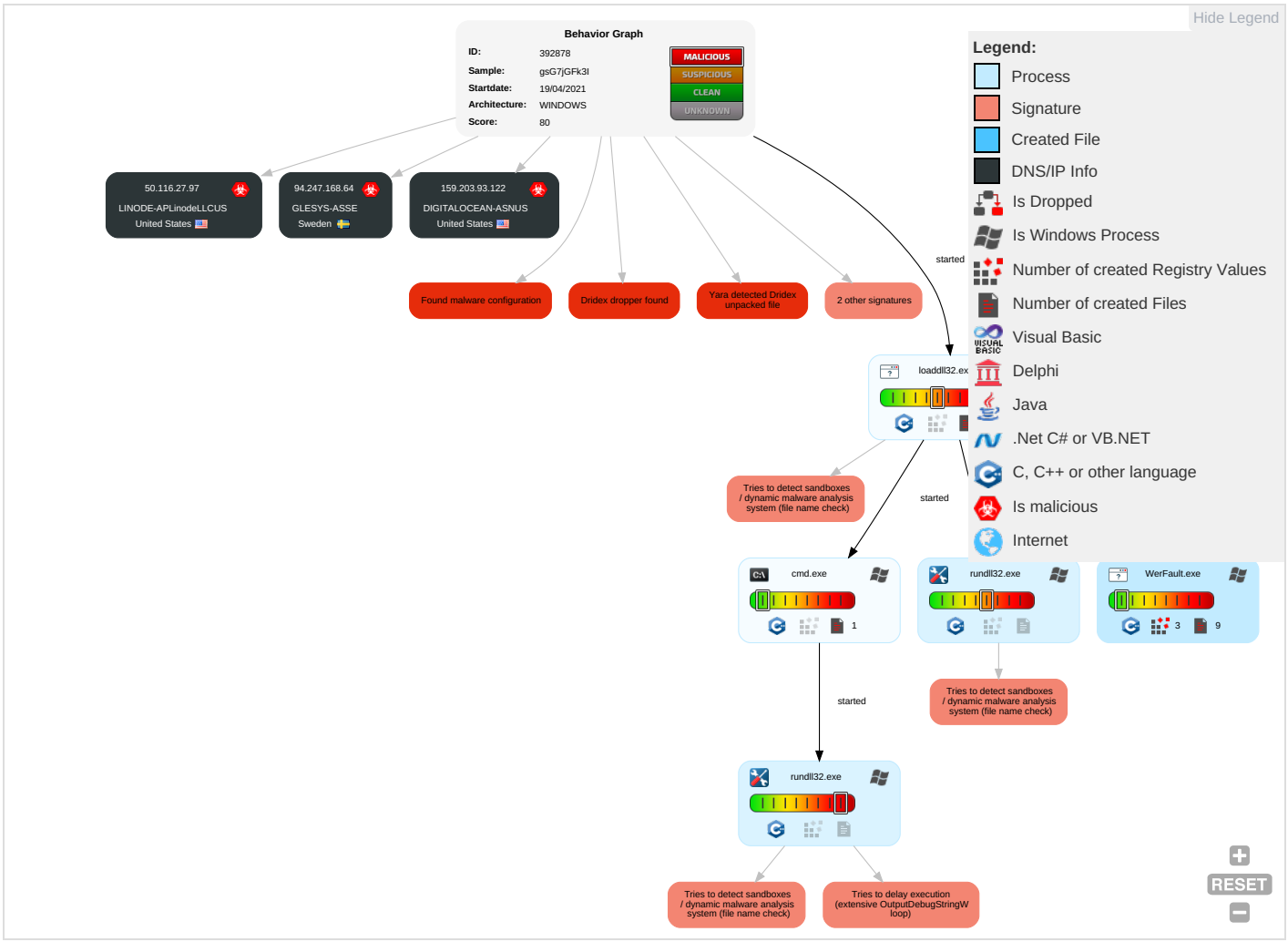
Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes / dynamic malware analysis system (file name check)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 3	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

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
gsG7jGFk3I.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.d50000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.2.loaddll32.exe.1390000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
5.2.rundll32.exe.5a0000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ansicon.adoxa.vze.com/6	gsG7jGFk3I.dll	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.203.93.122	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
50.116.27.97	unknown	United States		63949	LINODE-APLinodeLLCUS	true
94.247.168.64	unknown	Sweden		43948	GLESYS-ASSE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392878
Start date:	19.04.2021
Start time:	23:32:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gsG7jGFk3I (renamed file extension from none to 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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.bank.troj.evad.winDLL@8/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.5% (good quality ratio 50.6%) • Quality average: 80% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe

Simulations

Behavior and APIs

Time	Type	Description
23:33:21	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
159.203.93.122	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	6l18PHjcrE.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PoCqqwACRo.dll	Get hash	malicious	Browse	
50.116.27.97	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	6l18PHjcrE.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	
	PoCqqwACRo.dll	Get hash	malicious	Browse	
94.247.168.64	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTlVYi.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	
	9JXXdpfiQm.dll	Get hash	malicious	Browse	
	t4KzTUSzkx.dll	Get hash	malicious	Browse	
	POQ6m91rE7.dll	Get hash	malicious	Browse	
	6l18PHjcrE.dll	Get hash	malicious	Browse	
	4ryCxciDFA.dll	Get hash	malicious	Browse	
	PoCqqwACRo.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	15sV4KdrCN.dll	Get hash	malicious	Browse	• 159.203.93.122
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 159.203.93.122
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 159.203.93.122
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 159.203.93.122
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 159.203.93.122
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 159.203.93.122
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 159.203.93.122
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 159.203.93.122
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 159.203.93.122
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 159.203.93.122
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 159.203.93.122
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 159.203.93.122
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 159.203.93.122
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 159.203.93.122
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 159.203.93.122

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 159.203.93.122
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 159.203.93.122
	6l18PHjcrE.dll	Get hash	malicious	Browse	• 159.203.93.122
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 159.203.93.122
	PoCqqwACRo.dll	Get hash	malicious	Browse	• 159.203.93.122
LINODE-APLinodeLLCUS	15sV4KdrCN.dll	Get hash	malicious	Browse	• 50.116.27.97
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 50.116.27.97
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 50.116.27.97
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 50.116.27.97
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 50.116.27.97
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 50.116.27.97
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 50.116.27.97
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 50.116.27.97
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 50.116.27.97
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 50.116.27.97
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 50.116.27.97
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 50.116.27.97
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 50.116.27.97
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 50.116.27.97
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 50.116.27.97
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 50.116.27.97
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 50.116.27.97
	6l18PHjcrE.dll	Get hash	malicious	Browse	• 50.116.27.97
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 50.116.27.97
	PoCqqwACRo.dll	Get hash	malicious	Browse	• 50.116.27.97
GLESYS-ASSE	15sV4KdrCN.dll	Get hash	malicious	Browse	• 94.247.168.64
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 94.247.168.64
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 94.247.168.64
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 94.247.168.64
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 94.247.168.64
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 94.247.168.64
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 94.247.168.64
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 94.247.168.64
	1UmI5PSg3K.dll	Get hash	malicious	Browse	• 94.247.168.64
	9eYYTTlVYi.dll	Get hash	malicious	Browse	• 94.247.168.64
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 94.247.168.64
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 94.247.168.64
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 94.247.168.64
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 94.247.168.64
	9JXXdpfiQm.dll	Get hash	malicious	Browse	• 94.247.168.64
	t4KzTUSzkx.dll	Get hash	malicious	Browse	• 94.247.168.64
	POQ6m91rE7.dll	Get hash	malicious	Browse	• 94.247.168.64
	6l18PHjcrE.dll	Get hash	malicious	Browse	• 94.247.168.64
	4ryCxciDFA.dll	Get hash	malicious	Browse	• 94.247.168.64
	PoCqqwACRo.dll	Get hash	malicious	Browse	• 94.247.168.64

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\Report.wer	
Size (bytes):	9244
Entropy (8bit):	3.7599477570961812
Encrypted:	false
SSDEEP:	96:+XlXyiy9hAdC5Q56tpXIQcQ6c6n+hcEZcw3P+a+z+HbHgiG6eugtYsaV9w72oNEU:ZTHUb+hjbjuq/u7sNS274ltb2h
MD5:	CA637BF3C41F975ED966E82973B6127F
SHA1:	DB8D3B9D91A1EAF74859F3D34894D4A39BA54D1C
SHA-256:	96C329E1CCA8BE541F2724B02D2CCC4A61439ED2130BBE8A02AB6E299B3FD3BF
SHA-512:	D0ECED1B4804A532541EBB0276F4205883C8DCBD98951D022B82F935179AFAE1407D23BDA24F16C7BE5D3F3A00680F17F81AB588391691C8C339547D2BE993F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.3.3.7.4.0.0.8.4.9.8.4.0.1.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.e.4.0.7.7.3.3.-.6.e.d.3.-.4.4.5.c.-.8.e.e.d.-.c.6.6.f.a.9.f.8.e.5.8.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.4.7.f.2.4.b.1.-.4.5.2.5.-.4.8.9.4.-.b.e.f.d.-.c.4.6.3.7.5.a.b.d.1.1.2.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.b.0.-.0.0.0.1.-.0.0.1.7.-.c.f.7.0.-.4.8.f.d.a.e.3.5.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.4././.0.4.:.1.0.:.5.0.:.5.4.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Apr 20 06:33:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44142
Entropy (8bit):	2.055490315923451
Encrypted:	false
SSDEEP:	192:w0rJHyc+uDuMpxd9WZ/9rABq/YfceZoQJh6CshwChaQloiVa:hSc+uD3pxd9WLncfyQhshwCha6oMa
MD5:	EE022C7A80D19ED999BC496BD418109B
SHA1:	64E5A3D05611DF5B2EB322C4073ACC29352423AD
SHA-256:	1CAFD6DE99F4FADF8B28F33310F5B91BB463598A31FC151F3E22AD4A6C5BDD21
SHA-512:	F5BD06B489639F365A033BA01D34DA184CB2326884FBC34B611F417606D3DC772D5669952DED0863590F1F91C077993797A1D0EB3D4FAAA6851E3CC214D64D3
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....u~`.....U.....B.....GenuineIntelW.....T.....u~`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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):	8366
Entropy (8bit):	3.6883289707568223
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNifM6XKQ6YgKSU+Lgmf2S1ACpBg89bBnycqsferm:RrlsNik6XKQ6Y9SU+Lgmf2S1XBn3fj
MD5:	6508757CC3BB29AECC71F9C3F1BCE58D
SHA1:	9611C8227C94B977648BF80B2AFE83F21E26BCD1
SHA-256:	15E63D0FD3407E006E64B8C02AB74CA51823A11F9EBA97F516820054A708EE3D
SHA-512:	977797979492E733726C724195FD67C9827BACDD21FCF6A6730F22B70FB488FB69D35EFFBF80A443E3E4A21FDF26D10B7B8434E7D5C239E3C81CCA31F12853C
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.>.1.7.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4658
Entropy (8bit):	4.425136673788134
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp.xml	
SSDEEP:	48:cvIwSD8zs8JgtWl9YeWSC8Bk8fm8M4JVFFnS+q8v7G3KcQlcQw6UrrTd:uITf6zfSNHJdSK63Kkw68rTd
MD5:	EF60E3BA1169424447995C7677E86701
SHA1:	B12774F1D531A0FFFCA5EE5D3A6DB2C0C5E4EE77
SHA-256:	534759930EE6EF637059B387CA4F708AAC6C5BF5F13BE456533DC8F9109E4073
SHA-512:	4918E923A29534AF1C190AB59721450754C40446D111E20C9F1876A10E98EA6A82413302BB02D181DD43FD772738BD291F65EBDBA74857EFFA395A7BC9066895
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="954224" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.5485478259715135
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	gsG7jGFk3I.dll
File size:	163840
MD5:	e8675c9ab1bb95547b902176997e37a1
SHA1:	c088263ed0a68c8b9ffb092d41a53603ae25e69b
SHA256:	6934bf4b117408db966b2c8afc1adde7e8bbb2063b7a284727e44a28a6769bea
SHA512:	b283006770f8cc37bb15cc75b652df50f7c24fc59b385477ff2e623cd5bfee7cc7e8c8247d2dc976c59d401af8345f4a2c664e76cc89a10aa3be82e1fec3298c
SSDEEP:	3072:IWX2IjzzpM+PncPeY8+O3AU3HRIHPh3UGfXy0BHNkIv/ScbQQ2y0iNM0+y+N0tc:I42IfzNPnoeY8j3AsHGPXpHNj6rByM3
File Content Preview:	MZ.....@.....{}..{}..{}..{}...}..@.2..|..=.T..}....S.z|..@..._}..|...T|..V/C..|..V/E..|..Rich[}.....PE..L.....}`.....!.....f.....D.....P....@.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x424410
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x607DE4E4 [Mon Apr 19 20:15:32 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5

General

File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b84fd50f2389cfd5bd83e2cf062986d1

Entrypoint Preview

Instruction
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp edx, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
je 00007FBD20979FFBh
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1001	0x0	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2768c	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x340	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x14c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x25040	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x3c	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2356e	0x23600	False	0.761560015459	data	7.55877156847	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2842	0x2a00	False	0.791573660714	data	7.53164670284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x28000	0x3588	0x1600	False	0.783380681818	MMDF mailbox	7.34765964879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x340	0x400	False	0.390625	data	2.73456990044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x14c	0x200	False	0.62890625	data	4.21021599876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x2e0	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, OpenSemaphoreW, LoadLibraryExA, GetModuleHandleW, OutputDebugStringA, GetProfileSectionW
OPENGL32.dll	glTexSubImage1D
ole32.dll	CreateStreamOnHGlobal
USER32.dll	TranslateMessage
ADVAPI32.dll	RegLoadAppKeyW

Version Infos

Description	Data
LegalCopyright	Freeware
InternalName	ANSI32
FileVersion	1.66
CompanyName	Jason Hood
Comments	http://ansicon.adoxa.vze.com/
ProductName	ANSICON
ProductVersion	1.66
FileDescription	ANSI Console
OriginalFilename	ANSI32.dll
Translation	0x0409 0x04b0

Possible Origin

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

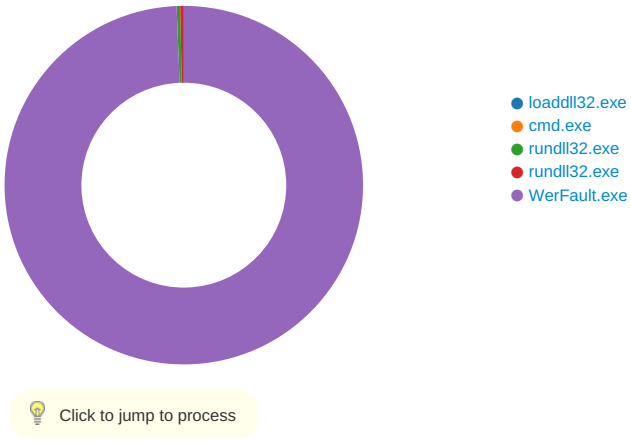
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 1712 Parent PID: 5788

General

Start time:	23:32:52
Start date:	19/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\gsG7jGFk3I.dll'
Imagebase:	0xb30000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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

Analysis Process: cmd.exe PID: 668 Parent PID: 1712

General

Start time:	23:32:52
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3I.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: rundll32.exe PID: 4832 Parent PID: 668

General

Start time:	23:32:52
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3I.dll',#1
Imagebase:	0xfc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.494850916.000000006E881000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6E895E36	ReadFile

Analysis Process: rundll32.exe PID: 4516 Parent PID: 1712

General

Start time:	23:33:20
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\gsG7jGFk3I.dll',ReadLogRecord
Imagebase:	0xfc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000005.00000002.495709984.000000006E881000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6E895E36	ReadFile

Analysis Process: WerFault.exe PID: 4480 Parent PID: 1712

General

Start time:	23:33:22
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1712 -s 428
Imagebase:	0xfb0000
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	6F761717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F75497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp.xml	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAC5.tmp.csv	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER35.tmp.txt	success or wait	1	6F75497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 ba 75 7e 60 a4 05 12 00 00 00 00 00	MDMP..... .....u~`.....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 bc 14 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 b0 06 00 00 94 75 7e 60 07 00 00 00 10 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B..... ..GenuineIntelW.....T... .....u~`..... .....0..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 88 6e a8 f4 b1 00 00 00 00 00 00 00 88 6e 00 00 88 6e 00 00 00 00 b4 f4 b1 00 00 00 88 6e 23 00 00 00 46 02 01 00 98 f4 b1 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+......n...........n...n.... ....n#...F.......+.........	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	168	04 17 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 6e 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 88 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 c0 17 00 00	...........................n.. ....n........	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	20	12 00 00 00 bc e6 b1 00 00 00 00 00 44 19 00 00 e0 26 00 00	...........D....&..	success or wait	18	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	6468	bc 9a 30 77 f2 1d 35 77 aa aa aa aa f0 e6 b1 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 44 ec b1 00 00 00 00 00 b0 01 00 00 00 00 00 00 00 00 00 00 b0 01 00 00 c4 01 00 00 88 e7 b1 00 aa aa aa aa 88 e7 b1 00 12 12 35 77 c4 01 00 00 00 00 00 00 aa aa aa aa ec e7 b1 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 78 e9 b1 00 28 e9 b1 00 c4 01 00 00 00 00 b9 02 aa aa aa aa ac 01 00 00 b4 01 00 00 b8 01 00 00 b0 01 00 00 00 00 00 00 b0 01 00 00 ac 01 00 00 b8 01 00 00 b4 01 00 00 aa aa aa aa 10 e7 b1 00 aa aa aa aa 3c e8 b1 00 f0 17 31 77 aa aa aa aa 00 00 00 00 a4 e7 b1 00 91 0c 35 77 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 68 f5 b1 00 3d ac 34 77 28 e9 b1 00 78 e9 b1 00 aa aa aa aa 00 00 00	..0w..5w...................... ..D.......................... ....5w............. ....x... (........................ .... <.....1w............. 5w...................h...=.4w (...x..........	success or wait	17	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	748	bc b1 30 77 d6 c9 2e 77 c8 00 00 00 aa aa aa aa 10 00 00 00 a8 fd 38 01 74 fe 38 01 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 aa aa aa aa 00 90 cf 00 00 90 cf 00 00 00 00 00 c8 00 00 00 aa aa aa aa c8 00 00 00 aa aa aa aa 00 90 cf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 ca e1 00 00 00 00 00 00 00 00 00 00 81 e0 00 00 d0 ce 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 d2 ce 00 70 fe 24 01 70 85 e0 00 78 fe 24 01 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..0w...w.............8.t.8... ..@..w@..w................... ....T...p. $.p...x.$.....................	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.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 00 00 00 00 00 00 00 00 00 00 88 6e 00 00 88 6e 00 00 00 00 00 e7 b1 00 bc 9a 30 77 23 00 00 00 16 02 00 00 c0 e6 b1 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.................n...n.... ......0w#..........+.........	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	48	d4 0a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 90 cf 00 00 00 00 00 14 fd 38 01 00 00 00 00 ec 02 00 00 9c 8f 00 00 cc 02 00 00 f0 22 00 00	....8... ...."..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	4	18 00 00 00	....	success or wait	24	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	32	1a 00 00 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 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	24	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	120	00 00 ce 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 f4 0e 64 17 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...v.....`..A!..-a..d......... ....B.......B?........... ....#............ ..@A.........................	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	34	1c 00 00 00 67 00 73 00 47 00 37 00 6a 00 47 00 46 00 6b 00 33 00 49 00 2e 00 64 00 6c 00 6c 00 00 00	....g.s.G.7.j.G.F.k.3.I...d.l.l...	success or wait	2	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	668	00 00 88 6e 00 00 00 00 00 10 02 00 00 00 00 00 72 49 67 60 9e 17 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 00 01 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 c0 c0 02 00 00 00 00 00 30 e8 02 00 00 00 00 fc 52 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 05 66 03 00 00 00 00 00 05 66 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a fb 15 00 00 00 00 00 e6 03 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 7e 44 0a 00 00 00 00 00 02 c3 de 47 00 00 00 00 c1 c7 e6 15 00 00 00 00 76 5a f5 0c 00 00 00 00 d5 26 cd 00 00 00 00 00 d8 96 00 00 df 92 00 00 e0 7f 04 00 24 2b 06 00 e6 03 0a 00 fb 7e 15 00 7e 44 0a 00 cd f9 22 00 9f 1c 01 00 be 2b 0e 00 00 00 00 00 f0 53 14 00 01 52 04	...n.....rIg`.....Zb ....0 .....R.....f.. .....f.....Z..... .....@.....~D.....G.... .....vZ.....&..... .....$+.....~..~D....".... .+.....S...R.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	6702	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 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	....F.i.l.e.....F.i.l.e..... ..F.i.l.e.....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..	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBB.tmp.dmp	unknown	120	03 00 00 00 c4 00 00 00 08 07 00 00 04 00 00 00 24 0a 00 00 d8 07 00 00 0e 00 00 00 3c 00 00 00 fc 11 00 00 05 00 00 00 24 01 00 00 bc 25 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 c8 10 00 00 ee 9b 00 00 15 00 00 00 ec 01 00 00 38 12 00 00 16 00 00 00 98 00 00 00 24 14 00 00	.....$.....<. .....$....%.....`... ....8.....T..... .....8.....$...	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.7.1.2.<./.P.i.d.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 35 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.8.5.8.6.<./.U.p.t.i.m.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 33 00 34 00 32 00 38 00 34 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.>.5.9.3.4.2.8.4.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 35 00 33 00 32 00 30 00 35 00 37 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.5.3.2.0.5.7.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 36 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.6.6.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 32 00 35 00 30 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.2.5.0.4.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 32 00 33 00 30 00 30 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.2.3.0.0.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.9.2.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.1.3.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.7.8.4.<./.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.5.1.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.9.6.4.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 30 00 34 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.9.0.4.6.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.8.9.6.4.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 32 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.2.9.2.<./.P.i.d.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 35 00 32 00 33 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.4.5.2.3.5.0.<./.U.p.t.i.m.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4..g.u.e.s.t.=.".0.".h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 35 00 32 00 32 00 35 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.>.5.2.2.5.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 31 00 31 00 33 00 39 00 34 00 38 00 31 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.>.1.1.1.3.9.4.8.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 30 00 38 00 33 00 35 00 33 00 32 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.>.1.0.0.8.3.5.3.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 35 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.7.5.2.8.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 38 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.>.9.3.8.8.8.8.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.5.6.0.<./.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.8.0.<./.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 39 00 34 00 30 00 39 00 32 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.4.0.9.2.8.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 34 00 30 00 30 00 37 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.4.0.0.7.9.3.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 39 00 34 00 30 00 39 00 32 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.4.0.9.2.8.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 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 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.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 69 00 61 00 6f 00 6a 00 67 00 6f 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.i.a.o.j.g.o.,. .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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 69 00 61 00 6f 00 6a 00 67 00 6f 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.i.a.o.j.g.o.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 31 00 37 00 32 00 38 00 32 00 35 00 31 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.>.1.5.6.1.7.2.8.2.5.1.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 42 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.B.<./.F.l.a.g.s.>.	success or wait	3	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 34 00 2d 00 32 00 30 00 54 00 30 00 36 00 3a 00 33 00 33 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.4.-.2.0.T.0.6.:.3.3.:.3.1.Z.".>.	success or wait	1	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 37 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 32 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 32 00 39 00 32 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.1.". .P.I.D.=.".1.7.1.2.". .U.p.t.i.m.e.M.S.=.".2.9.2.3. 4.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".2.9.2.3.4.". .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	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 65 00 34 00 30 00 37 00 37 00 33 00 33 00 2d 00 36 00 65 00 64 00 33 00 2d 00 34 00 34 00 35 00 63 00 2d 00 38 00 65 00 65 00 64 00 2d 00 63 00 36 00 36 00 66 00 61 00 39 00 66 00 38 00 65 00 35 00 38 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.e.4.0.7.7.3.3.-.6.e.d.3.-.4.4.5.c.-.8.e.e.d.-.c.6.6.f.a.9.f.8.e.5.8.d.<./.G.u.i.d.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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 34 00 2d 00 32 00 30 00 54 00 30 00 36 00 3a 00 33 00 33 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.2.0.T.0.6.:.3.3.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4FA.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	6F75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD7.tmp.xml	unknown	4658	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	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\Report.wer	unknown	2	ff fe	..	success or wait	1	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\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	149	6F75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_eac5c5ff6135a0fa57fda95e87d917a4681d1_160cf2be_11c400b1\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 39 00 30 00 31 00 35 00 31 00 32 00 39 00 34 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.9.0.1.5.1.2.9.4.3.	success or wait	1	6F75497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{26ee909c-7281-f919-18b6-371b26234f34}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F771FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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 00 00 88 6E 02 00 00 00 08 00 00 00 00 00 88 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6F771FE8	RegSetValueExW

Disassembly

Code Analysis