ID: 413039
Sample Name: a98ab505_by_Libranalysis.dll
Cookbook: default.jbs
Time: 06:54:07
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

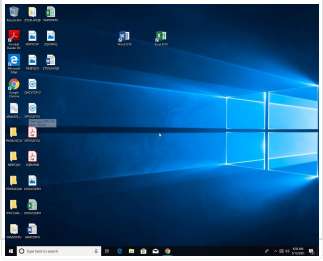
Analysis Report a98ab505_by_Libranalysis.dll

Overview

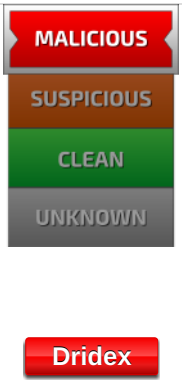
General Information

Sample Name:	a98ab505_by_Libranalysis.dll
Analysis ID:	413039
MD5:	a98ab505ecc3ec...
SHA1:	ff5d7193d073303..
SHA256:	cf3a3944a4a37b5.
Infos:	

Most interesting Screenshot:



Detection

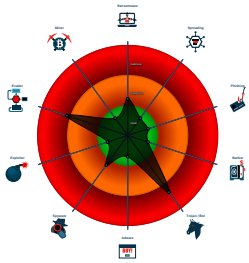


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes / dynamic…
- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6636 cmdline: loaddll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6644 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6656 cmdline: rundll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6688 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6656 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "BwjTiXD0nMT8wuL0lzuDMT1lwajgYLnSPMpMch1H2fk8H",
    "duBYwiNAKNjPWhQIWm9t4nFdK0AZ0qg5qRVUphxjgPm8fOpLdTGQDOkY8vper"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.755906569.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

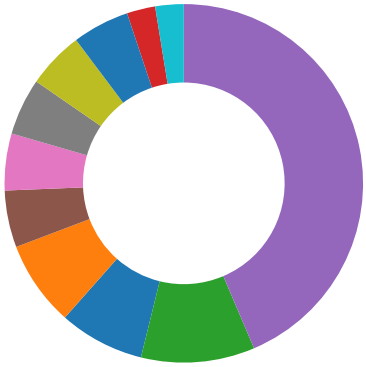
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.10000000.3.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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

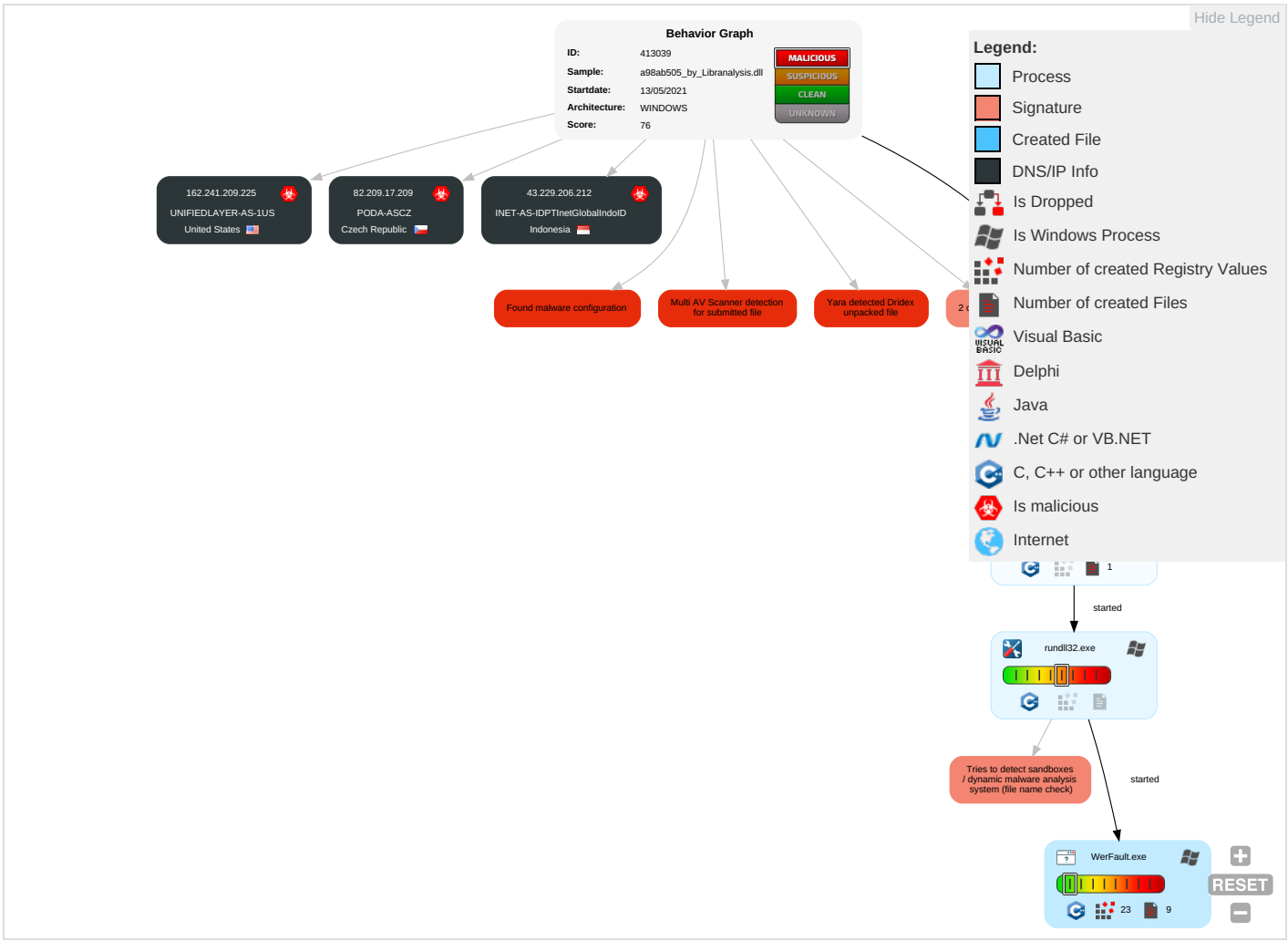
Malware Analysis System Evasion:

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 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 1 2 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 1 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	Account 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 2	LSA Secrets	System Owner/User 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	Remote System 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 1	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
a98ab505_by_Libranalysis.dll	49%	ReversingLabs	Win32.Trojan.Convagent	
a98ab505_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.3490000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	

Domains and IPs

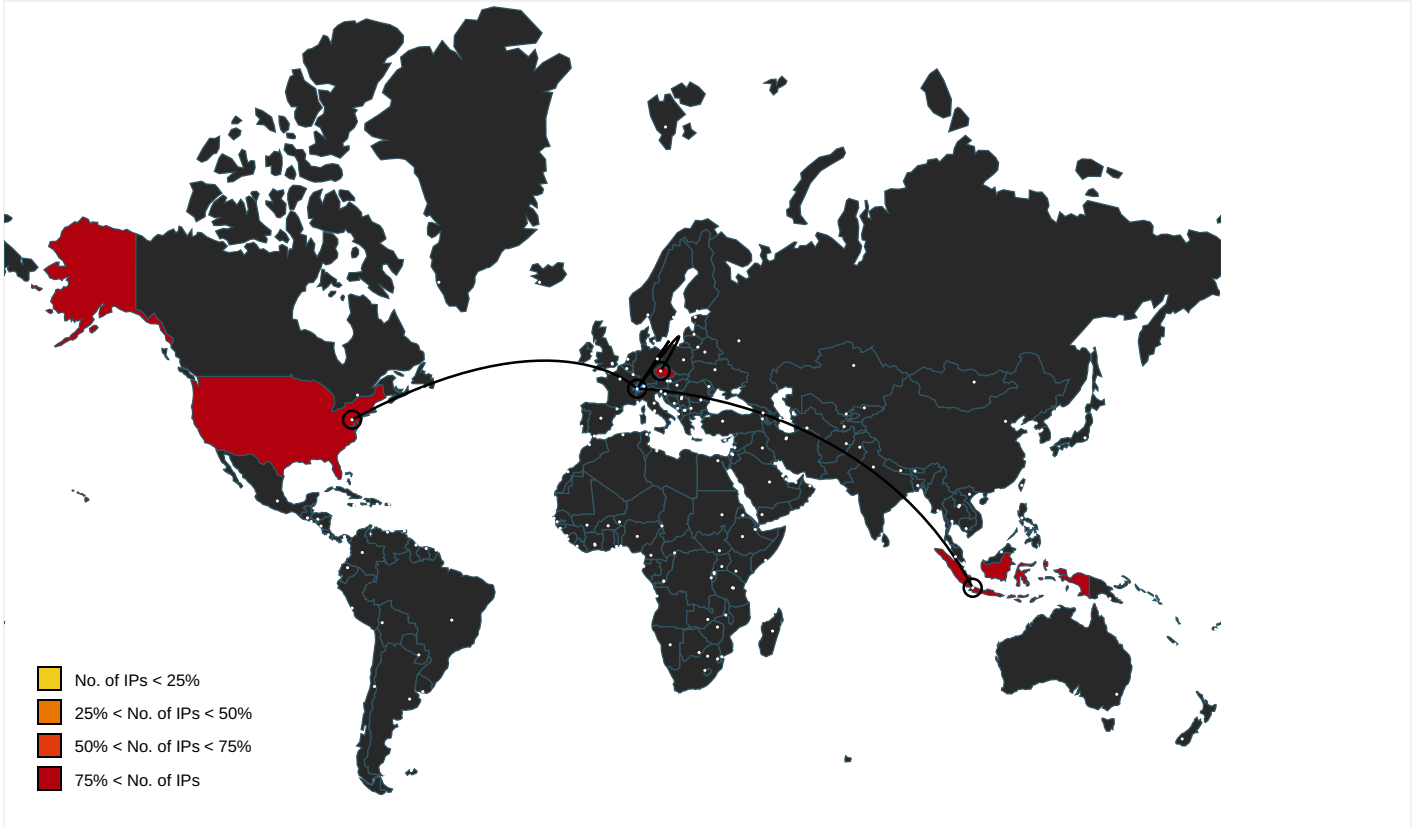
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro	WerFault.exe, 0000000E.0000000 3.748855263.000000000456C000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.209.17.209	unknown	Czech Republic		30764	PODA-ASCZ	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.209.225	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
43.229.206.212	unknown	Indonesia		24532	INET-AS-IDPTInetGlobalIndoID	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413039
Start date:	13.05.2021
Start time:	06:54:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a98ab505_by_Libranalysis.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 68.1% (good quality ratio 48.1%) • Quality average: 49.5% • Quality standard deviation: 39.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
UNIFIEDLAYER-AS-1US	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12680
Entropy (8bit):	3.768336391710609
Encrypted:	false
SSDEEP:	192:u7EbZiN0oXruHBUZMX4jed+sQR/u7sHS274ltWci:SKZiDXaBUZMX4jea/u7sHX4ltWci
MD5:	E08CBB1D441D88BDE4065ACAF4011018

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\Report.wer	
SHA1:	F3484E678D6F0365DEC61113308FC2B73786EBBA
SHA-256:	2CC5AA0258F78DBA838ACE173AB8661168795596EF822389C57AE0213BE3A78D
SHA-512:	B4346D751029D57B6A8D038475C45B348C760730CBF15C5DE49771892206E7E28B01C2453763D7D0BB2BBAAD8F14284BFBFF82D852283B0B2F147A1E58989E95
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.5.5.3.3.5.2.5.3.0.0.2.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.5.5.3.4.2.2.5.2.9.8.1.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.b.f.f.1.c.7.c.-.a.6.5.a.-.4.c.3.1.-.b.f.8.a.-.f.b.e.d.a.5.8.4.5.2.5.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.7.8.9.3.9.2.3.-.8.b.8.9.-.4.6.3.8.-.8.5.6.3.-.4.3.8.0.a.7.2.1.5.3.8.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.0.0.-.0.0.0.1.-.0.0.1.b.-.b.d.7.7.-.f.5.2.0.b.4.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 04:55:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	41624
Entropy (8bit):	2.4051390385270874
Encrypted:	false
SSDEEP:	192:JbEHKHzvZNzNUNNN6qAmWtjjRNnD9NZWWAogMboc/MyO7/5p0EMZmVzZVjnkwEnz:KHkZNzNUNNNJEpV3ZWWhF1anXZVjnHEz
MD5:	5D86A78862C271FFAA90AF0B090594CD
SHA1:	75C3193765597FC6EBE2855FAACB36866FF7571F
SHA-256:	8FFF2A44A9EE0A10E2E764F4DA7073546711C70E742A7EDB20A6266A623548AB
SHA-512:	95F7A2DC53E22210017F17FE32DB6BDDAB314ECA9C3C21B5906169D225EAFF6A64D298A7AB8F10601AD2371376CF7A9BC711D3024265F298EE2AA92BB115317
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....H..`.....U.....B.....P .....GenuineIntelW.....T.....$..`.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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):	8294
Entropy (8bit):	3.6953177362699807
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiO36XX6Yr66pQgmfTpvS++prm89b0ysfHEY8m:RrlsNi26n6Ym6pQgmfTBSt0xfHV
MD5:	CF068ADA221E4144E98A7872F3875885
SHA1:	C754910C932EF8CDD8DA8910C5FD06DA571933F8
SHA-256:	D326B9BE4CD1C7E1BADFEBABF355930A4A46FDC3646888A686D93EC73815AF73
SHA-512:	E76CF7FB5666E54C6233CFD6F1A46DBB5EB9903F74CC553E5F4B5432438CC329A8B069CD57DB6CEDD88EF9F98723F88A08B976D3E26C73B982D0FFBC56623C7
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4663
Entropy (8bit):	4.475899785195257
Encrypted:	false
SSDEEP:	48:cvIwSD8zs4JgtWI9K1yWSC8Bu8fm8M4JCdsHNbF9V2+q8/KNFVBn4SrSmd:uITf+tVSNZJ9NN2NNlDWmd
MD5:	C2832FDD823216C133067E69989034B6
SHA1:	86AF26EB5AAE25548EF6B32DF32AA407F57CCE02
SHA-256:	E8125B9BCB4F2AF73338A4B3A7F5B93480FE172C75E42BDBB9B03F1890E396F3
SHA-512:	CF57A45D53AC98FFF9652C27F48600583753A42E4DC1191E2229792C45BA64A4A17A6E5E8F1F6FFF6050004F8CA70ACAE166DBD045512501897 55B4362844F1B

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp.xml	
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="987246" />.. <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):	7.567246231271622
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:	a98ab505_by_Libranalysis.dll
File size:	160256
MD5:	a98ab505ecc3ec9d5c5d4571f4a2b5fe
SHA1:	ff5d7193d073303d7821ea418a7fdede1a62d384
SHA256:	cf3a3944a4a37b5c13842e1acc85b10a69dddb1b1c9c7de2a432b4ba32bb1781
SHA512:	0b085611813d868957edd720be45332ee6ebf1b8ce86111880a29181657c02395ed5e3b2745cf356ff910bbab0ed7b6c5084544f8fbaf4b21a32302134bcbcbc
SSDEEP:	3072:dyqDAKfnwLu67wJfAXzgAV12yo1DxbJ6rcKyMYK4f:3aiuwJ6zLV1/Sll5KM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.%.0zK.0zK.0zK.0zJ.}{K...3..{K.....P{K...3..zK.V....zK...1..{K.....zK.Rich0zK.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10022f50
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F8E [Thu May 13 01:23:26 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	c9d8b256fabdf7ec02ac0e021f0f72c6

Entrypoint Preview

Instruction
xor eax, eax
add eax, 00002234h
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 eax, 02h
jne 00007F1360D795A9h
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
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

Rich Headers

Programming Language:	[RES] VS2012 UPD3 build 60610 [LNK] VS2005 build 50727 [EXP] VS2005 build 50727 [C] VS2012 UPD4 build 61030 [IMP] VS2013 UPD2 build 30501

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2672a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x267f8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2b000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2c000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x220cc	0x22200	False	0.762248168498	data	7.58982753446	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x2a76	0x2c00	False	0.791548295455	data	7.46837367369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x27000	0x3324	0x1800	False	0.7353515625	MMDF mailbox	7.23030774842	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x3a0	0x400	False	0.423828125	data	3.05991849143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x240	0x400	False	0.5078125	data	4.04632895522	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2b060	0x33c	data		

Imports

DLL	Import
CLUSAPI.dll	ClusterEnum
ADVAPI32.dll	RegOverridePredefKey
RASAPI32.dll	RasGetConnectionStatistics
KERNEL32.dll	LoadLibraryExA, LoadLibraryW, GetProfileSectionW, GetProfileSectionA, OpenSemaphoreW, CreateFileW, CloseHandle, OutputDebugStringA
OPENGL32.dll	glTexSubImage1D
USER32.dll	TranslateMessage
ole32.dll	CreateStreamOnHGlobal, CreatePointerMoniker

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	x2otfb
FileVersion	7.2.5422.00
Full Version	7.2.5_000-b00
CompanyName	Oracle Corporation
ProductName	Xhot(BM) Ltloehey YO 8
ProductVersion	7.2.5422.00
FileDescription	Java(TM) Platform SE binary
OriginalFilename	x2otfb.dll
Translation	0x0000 0x04b0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:54:54.167156935 CEST	59123	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:54.198420048 CEST	54531	53	192.168.2.4	8.8.8.8

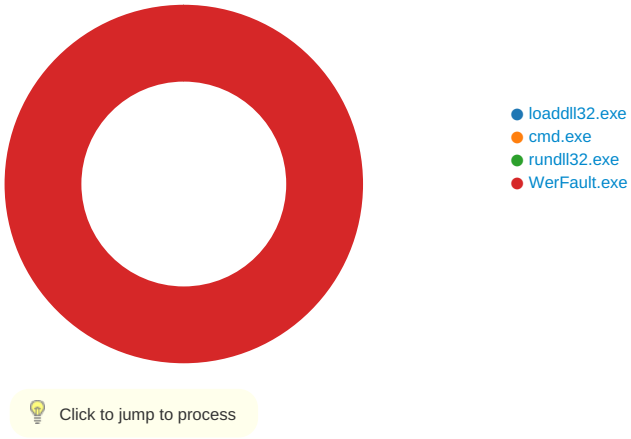
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:54:54.216065884 CEST	53	59123	8.8.8.8	192.168.2.4
May 13, 2021 06:54:54.263489008 CEST	53	54531	8.8.8.8	192.168.2.4
May 13, 2021 06:54:55.249706984 CEST	49714	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:55.313155890 CEST	53	49714	8.8.8.8	192.168.2.4
May 13, 2021 06:54:56.890480042 CEST	58028	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:56.939775944 CEST	53	58028	8.8.8.8	192.168.2.4
May 13, 2021 06:54:57.243531942 CEST	53097	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:57.301326990 CEST	53	53097	8.8.8.8	192.168.2.4
May 13, 2021 06:54:58.328294992 CEST	49257	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:58.377069950 CEST	53	49257	8.8.8.8	192.168.2.4
May 13, 2021 06:54:59.805485010 CEST	62389	53	192.168.2.4	8.8.8.8
May 13, 2021 06:54:59.858119965 CEST	53	62389	8.8.8.8	192.168.2.4
May 13, 2021 06:55:01.073297024 CEST	49910	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:01.124840975 CEST	53	49910	8.8.8.8	192.168.2.4
May 13, 2021 06:55:01.915004015 CEST	55854	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:01.966907024 CEST	53	55854	8.8.8.8	192.168.2.4
May 13, 2021 06:55:03.454873085 CEST	64549	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:03.506932020 CEST	53	64549	8.8.8.8	192.168.2.4
May 13, 2021 06:55:04.271562099 CEST	63153	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:04.320266008 CEST	53	63153	8.8.8.8	192.168.2.4
May 13, 2021 06:55:05.399990082 CEST	52991	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:05.462759972 CEST	53	52991	8.8.8.8	192.168.2.4
May 13, 2021 06:55:06.794656038 CEST	53700	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:06.843369007 CEST	53	53700	8.8.8.8	192.168.2.4
May 13, 2021 06:55:07.569686890 CEST	51726	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:07.618385077 CEST	53	51726	8.8.8.8	192.168.2.4
May 13, 2021 06:55:08.429094076 CEST	56794	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:08.477752924 CEST	53	56794	8.8.8.8	192.168.2.4
May 13, 2021 06:55:10.104027987 CEST	56534	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:10.155740976 CEST	53	56534	8.8.8.8	192.168.2.4
May 13, 2021 06:55:11.468683004 CEST	56627	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:11.517378092 CEST	53	56627	8.8.8.8	192.168.2.4
May 13, 2021 06:55:12.531749010 CEST	56621	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:12.580511093 CEST	53	56621	8.8.8.8	192.168.2.4
May 13, 2021 06:55:13.800578117 CEST	63116	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:13.852796078 CEST	53	63116	8.8.8.8	192.168.2.4
May 13, 2021 06:55:18.835875988 CEST	64078	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:18.886480093 CEST	53	64078	8.8.8.8	192.168.2.4
May 13, 2021 06:55:19.925559044 CEST	64801	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:19.976767063 CEST	53	64801	8.8.8.8	192.168.2.4
May 13, 2021 06:55:30.666755915 CEST	61721	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:30.725814104 CEST	53	61721	8.8.8.8	192.168.2.4
May 13, 2021 06:55:40.182075024 CEST	51255	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:40.240514040 CEST	53	51255	8.8.8.8	192.168.2.4
May 13, 2021 06:55:43.561554909 CEST	61522	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:43.613298893 CEST	53	61522	8.8.8.8	192.168.2.4
May 13, 2021 06:55:48.212294102 CEST	52337	53	192.168.2.4	8.8.8.8
May 13, 2021 06:55:48.276665926 CEST	53	52337	8.8.8.8	192.168.2.4
May 13, 2021 06:56:00.218456984 CEST	55046	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:00.305618048 CEST	53	55046	8.8.8.8	192.168.2.4
May 13, 2021 06:56:00.896776915 CEST	49612	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:01.003010035 CEST	53	49612	8.8.8.8	192.168.2.4
May 13, 2021 06:56:01.596420050 CEST	49285	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:01.653580904 CEST	53	49285	8.8.8.8	192.168.2.4
May 13, 2021 06:56:02.005770922 CEST	50601	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:02.070842028 CEST	53	50601	8.8.8.8	192.168.2.4
May 13, 2021 06:56:02.083420992 CEST	60875	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:02.170087099 CEST	53	60875	8.8.8.8	192.168.2.4
May 13, 2021 06:56:02.737278938 CEST	56448	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:02.795300961 CEST	53	56448	8.8.8.8	192.168.2.4
May 13, 2021 06:56:03.457828045 CEST	59172	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:03.514831066 CEST	53	59172	8.8.8.8	192.168.2.4
May 13, 2021 06:56:03.961601019 CEST	62420	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:04.018767118 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:56:04.774547100 CEST	60579	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:04.831553936 CEST	53	60579	8.8.8.8	192.168.2.4
May 13, 2021 06:56:05.651005983 CEST	50183	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:05.749567032 CEST	53	50183	8.8.8.8	192.168.2.4
May 13, 2021 06:56:06.284044027 CEST	61531	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:06.341527939 CEST	53	61531	8.8.8.8	192.168.2.4
May 13, 2021 06:56:11.352149010 CEST	49228	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:11.411710024 CEST	53	49228	8.8.8.8	192.168.2.4
May 13, 2021 06:56:47.638673067 CEST	59794	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:47.695739031 CEST	53	59794	8.8.8.8	192.168.2.4
May 13, 2021 06:56:49.312550068 CEST	55916	53	192.168.2.4	8.8.8.8
May 13, 2021 06:56:49.377916098 CEST	53	55916	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6636 Parent PID: 5860

General

Start time:	06:54:59
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll'
Imagebase:	0xe20000
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: 6644 Parent PID: 6636

General

Start time:	06:55:00
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll',#1
Imagebase:	0x11d0000
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: 6656 Parent PID: 6644

General

Start time:	06:55:00
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\a98ab505_by_Libranalysis.dll',#1
Imagebase:	0xd10000
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: 00000002.00000002.755906569.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6688 Parent PID: 6656

General

Start time:	06:55:31
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6656 -s 764
Imagebase:	0xae0000
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	6F571717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F56497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9C1.tmp.csv	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE65.tmp.txt	success or wait	1	6F564BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 48 b1 9c 60 a4 05 12 00 00 00 00 00	MDMP..... .....H..`.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.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 50 20 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 00 1a 00 00 24 b1 9c 60 08 00 00 00 12 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 3d 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......P .... ..GenuineIntelW...........T... ....$..`.................. ....0..=..............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.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 00 00 df 91 01 10 20 35 64 03 ff ff ff ff df 91 01 10 3b 32 00 02 54 f9 27 03 df 91 01 10 23 00 00 00 03 02 01 00 d0 f8 27 03 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........... 5d.........;2.. T.'.....#.........'.+.........	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	168	04 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 df 91 01 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a 26 00 00	....Z&..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	20	0c 00 00 00 d8 f5 43 03 00 00 00 00 28 0a 00 00 82 2f 00 00	......C.....(..../..	success or wait	12	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	2600	bc b1 11 77 d6 c9 0f 77 64 02 00 00 aa aa aa aa 10 00 00 00 6c f6 43 03 38 f7 43 03 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 10 07 64 03 00 20 11 03 00 20 11 03 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 20 11 03 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa 60 bd 63 03 00 00 00 00 00 00 00 00 b0 08 64 03 00 c0 10 03 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 07 64 03 00 00 00 00 aa aa aa aa aa aa aa aa 54 c2 10 03 54 c2 10 03 48 07 64 03 48 07 64 03 00 00 00 00 aa aa aa aa 10 07 64 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wd...........l.C.8.C... ..@..w@..w..d.. ... .d... ....d........ ....`.c... ....d..................... ....d.............T...T. ..H.d.H.d...........d.........	success or wait	11	6F56497A	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp</td><td>unknown</td><td>256</td><td>8b f9 c7 07 00 00 00 00 8d 77 04 8b 06 85 c0 74 03 c6 00 00 8d 6f 0c 8b 45 00 85 c0 74 03 c6 00 00 8d 5f 14 8b 03 85 c0 74 03 c6 00 00 8d 47 1c 89 44 24 1c 8b 00 85 c0 74 03 c6 00 00 8b 44 24 50 85 c0 0f 84 56 01 00 00 80 38 00 0f 84 4d 01 00 00 6a 00 50 8d 4c 24 14 e8 ff 4d ff ff 8b 4c 24 0c 6a 3a 5a 89 0c 24 e8 38 5a ff ff 85 c0 74 10 80 78 01 2f 75 0a 80 78 02 2f 0f 84 28 01 00 00 6a 2f 5a 8b 0c 24 e8 19 5a ff ff 89 44 24 04 83 7c 24 04 00 74 3b 6a 3f 5a 8b c8 e8 04 5a ff ff 89 44 24 08 83 7c 24 08 00 74 14 ff 74 24 08 8b 4c 24 20 e8 e0 4d ff ff 8b 44 24 08 c6 00 00 8b cb ff 74 24 04 e8 ce 4d ff ff 8b 44 24 04 c6 00 00 6a 3a 5a 8b 0c 24 e8 c8 59 ff ff 89 44 24 04 83 7c 24 04 00 74 20 6a 00 8d 4c 24 20 8d 50 01 e8 b3 58 ff ff 8d 4c 24 1c e8 92 56 ff ff</td><td>.........w.....t.....o..E...t.
...._.....t.....G..D$.....t...
..D$P....V....8...M...j.P.L$..
.M...L$.j:Z..$.8Z....t..x./u..
x./..(...j/Z..$..Z...D$..|$..t;j?
Z....Z...D$..|$..t..t$..L$
..M...D$.......t$...M...D$....
j:Z..$..Y...D$..|$..t j..L$ .P
...X...L$...V..</td><td>success or wait</td><td>1</td><td>6F56497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp</td><td>unknown</td><td>4</td><td>02 00 00 00</td><td>....</td><td>success or wait</td><td>2</td><td>6F56497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp</td><td>unknown</td><td>716</td><td>3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa df 91 01 10 00 00 00 00 68 ea 27 03 bc 9a 11 77 23 00 00 00 06 02 00 00 d8 e8 27 03 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</td><td>?............................
....
....
....
....................+...S...+.
..+...........................
h.'....w#.........'.+.........
....
..............</td><td>success or wait</td><td>2</td><td>6F56497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp</td><td>unknown</td><td>48</td><td>18 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 20 11 03 00 00 00 00 d8 f5 43 03 00 00 00 00 28 0a 00 00 82 2f 00 00 cc 02 00 00 f2 2b 00 00</td><td>........ ....C.....
(..../.......+..</td><td>success or wait</td><td>1</td><td>6F56497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp</td><td>unknown</td><td>4</td><td>35 00 00 00</td><td>5...</td><td>success or wait</td><td>53</td><td>6F56497A</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	53	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	752	00 00 74 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 40 26 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 f0 a8 02 00 00 00 00 00 70 19 03 00 00 00 00 3e 60 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 14 7c 03 00 00 00 00 00 2a 7c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7c 0d 1b 00 00 00 00 00 c4 f1 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 f4 19 05 00 00 00 00	..ts.....0...U..s@..@&.....B.....B?.....#.....@A.....Zb.....p.....>`.....|.....*|.....|.....@.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	10850	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 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 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t.....F.i.l.e.....F.i.l.e...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF22.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 be 2e 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 80 84 00 00 15 00 00 00 ec 01 00 00 cc 1d 00 00 16 00 00 00 98 00 00 00 b8 1f 00 00	....d.....`...l..... .....T.....8..... ....T.....`.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.5.6.<./.P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 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	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 39 00 31 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.>.3.6.9.1.6.<./.U.p.t.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 38 00 33 00 31 00 34 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.1.4.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 33 00 30 00 33 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.0.3.1.0.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 32 00 37 00 35 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.5.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 39 00 33 00 31 00 38 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.3.1.8.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 39 00 33 00 31 00 38 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.3.1.8.4.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 38 00 36 00 36 00 34 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.>.1.8.6.6.4.8.<./.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 38 00 36 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.4.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 36 00 34 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.>.3.0.6.4.0.<./.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.3.6.8.<./.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 35 00 33 00 31 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.5.3.1.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.7.1.9.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 35 00 33 00 31 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.5.3.1.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.4.4.<./.P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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.>.c.m.d...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 37 00 32 00 34 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.7.2.4.4.<./.U.p.t.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 32 00 31 00 32 00 39 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.2.9.7.9.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 31 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 33 00 37 00 33 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.1.4.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 33 00 34 00 38 00 35 00 36 00 39 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.>.3.4.8.5.6.9.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	112	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 34 00 30 00 39 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 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.>.4.0.9.6.0.<./.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	106	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 34 00 39 00 35 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.>.4.9.5.2.<./.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 32 00 33 00 35 00 35 00 32 00 30 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.>.2.3.5.5.2.0.0.</.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 33 00 36 00 30 00 38 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.0.8.5.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 32 00 33 00 35 00 35 00 32 00 30 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.>.2.3.5.5.2.0.0.</.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 75 00 75 00 61 00 72 00 61 00 71 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.u.u.a.r.a.q.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 75 00 75 00 61 00 72 00 61 00 71 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.u.u.a.r.a.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 32 00 38 00 30 00 35 00 37 00 31 00 34 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.>.1.5.6.2.8.0.5.7.1.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 35 00 2d 00 31 00 33 00 54 00 30 00 34 00 3a 00 35 00 35 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.0.4.:.5.5.:.3.7.Z.".>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 36 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 36 00 35 00 36 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 38 00 34 00 33 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 38 00 34 00 33 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.=.".3.6.4.". .P.I.D.=.".6.6.5.6.". .U.p.t.i.m.e.M.S.=.".2.9.8.4.3.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.9.8.4.3.". .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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 62 00 66 00 66 00 31 00 63 00 37 00 63 00 2d 00 61 00 36 00 35 00 61 00 2d 00 34 00 63 00 33 00 31 00 2d 00 62 00 66 00 38 00 61 00 2d 00 66 00 62 00 65 00 64 00 61 00 35 00 38 00 34 00 35 00 32 00 35 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.b.f.f.1.c.7.c.-.a.6.5.a.-.4.c.3.1.-.b.f.8.a.-.f.b.e.d.a.5.8.4.5.2.5.6.<./.G.u.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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 35 00 2d 00 31 00 33 00 54 00 30 00 34 00 3a 00 35 00 35 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.0.4.:.5.5.:.3.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC695.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	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9B3.tmp.xml	unknown	4663	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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\Report.wer	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\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	184	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_d1933e54dec77ed372db99aebc0b4554f9da850_82810a17_1a60e121\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 37 00 30 00 31 00 30 00 30 00 34 00 34 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.7.0.1.0.0.4.4.4.8.	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6F5836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F581FB2	RegCreateKeyExW
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F5836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6F5836BF	unknown
\REGISTRY\A\{9bd45db3-6753-85e0-a626-ac86b35801c6}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6F5836BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 DF 91 01 10 02 00 00 00 01 00 00 00 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6F581FE8	RegSetValueExW

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

Disassembly

Code Analysis