ID: 413053
Sample Name:
cdc733ac_by_Libranalysis.dll
Cookbook: default.jbs
Time: 07:16:27
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

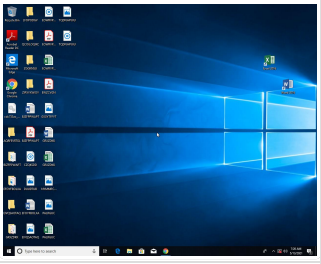
Analysis Report cdc733ac_by_Libranalysis.dll

Overview

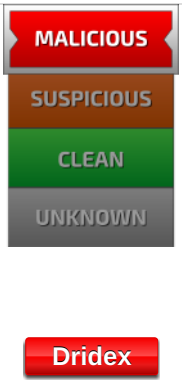
General Information

Sample Name:	cdc733ac_by_Libranalysis.dll
Analysis ID:	413053
MD5:	cdc733ac9b6d09...
SHA1:	197fd7c03f39db9..
SHA256:	31852f33db8ce7a.
Infos:	

Most interesting Screenshot:



Detection

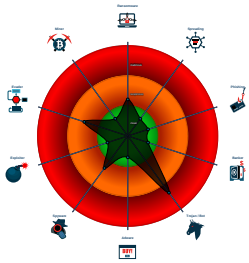


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…
- Internet Provider seen in connection…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 3336 cmdline: loaddll32.exe 'C:\Users\user\Desktop\cdc733ac_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2964 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\cdc733ac_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1188 cmdline: rundll32.exe 'C:\Users\user\Desktop\cdc733ac_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1188 -s 768 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": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvpltFNCpvA5goSylkxjIBtIwWPTv1DPbNEcuIekQC7O"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.325845384.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

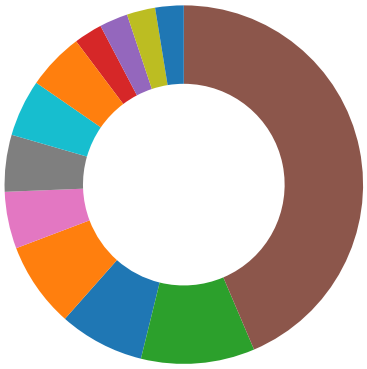
Unpacked PEs

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
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

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:

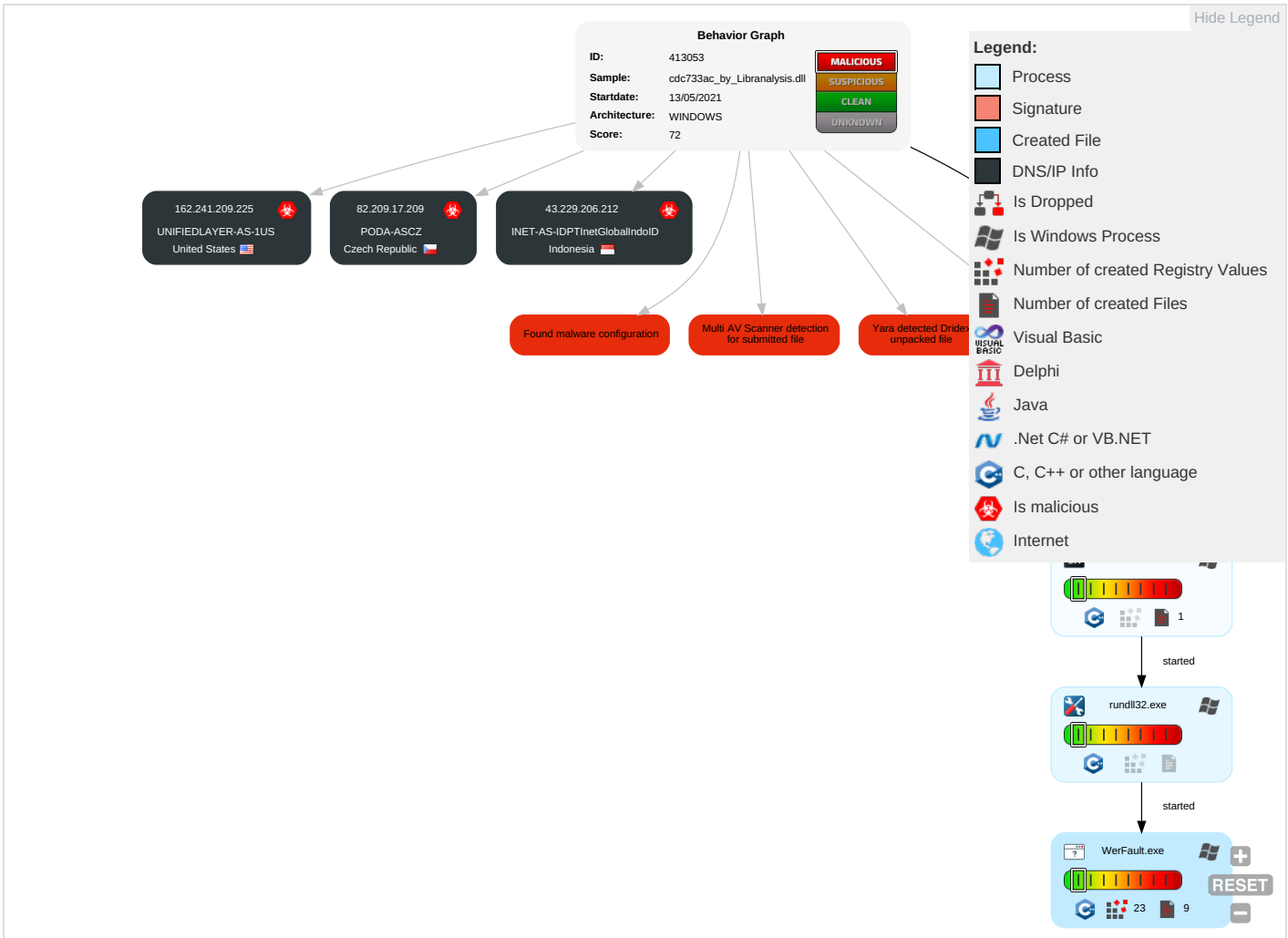
Yara detected Dridex unpacked file

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	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	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	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
cdc733ac_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
cdc733ac_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.3450000.2.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

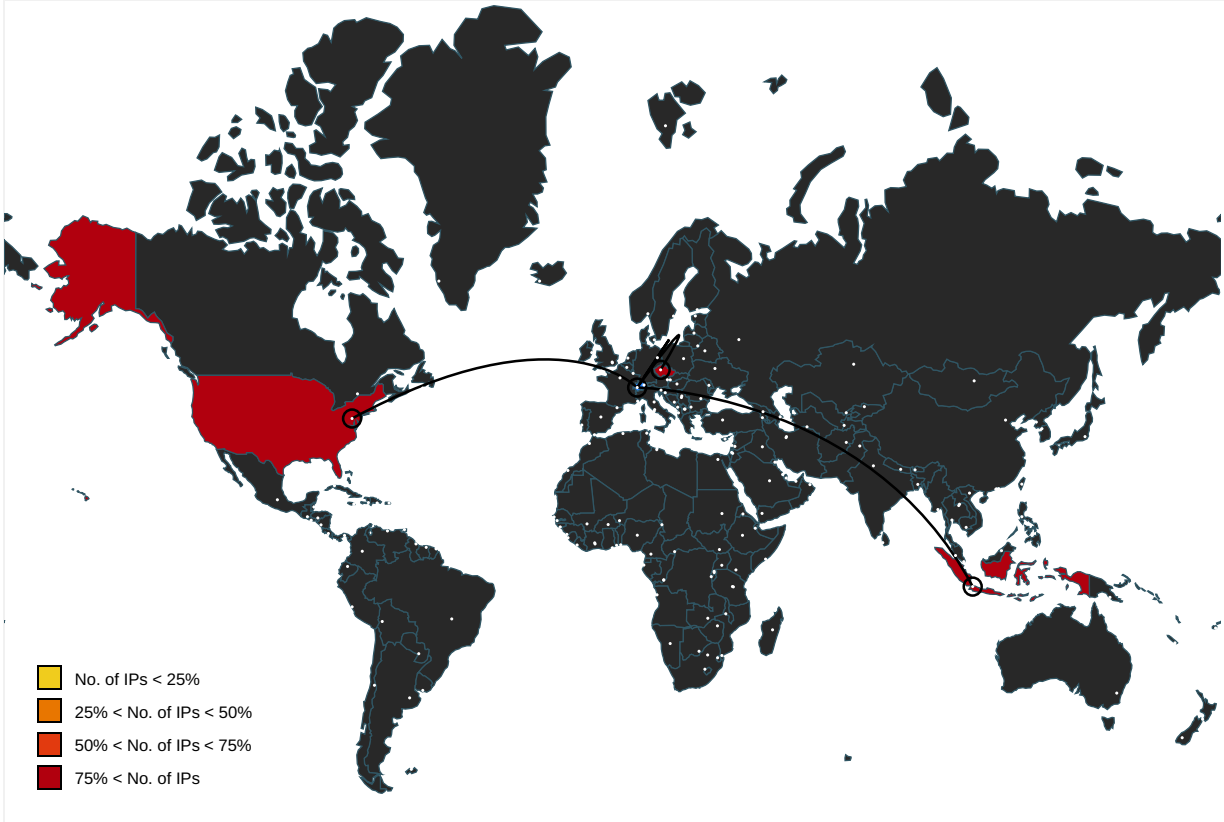
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro	WerFault.exe, 0000000E.0000000 3.320188440.0000000000DE1000.0 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
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:	413053
Start date:	13.05.2021
Start time:	07:16:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cdc733ac_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:	33
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:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.1% (good quality ratio 85.6%) • Quality average: 67.1% • Quality standard deviation: 35.1%
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	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_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
INET-AS-IDPTInetGlobalIndoID	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6bea48e8_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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12484
Entropy (8bit):	3.767235303442378
Encrypted:	false
SSDEEP:	192:qzij0oXccHBUZMX4jed+KG/u7snS274ltWc1:ui9XXBUZMX4jeu/u7snX4ltWc1
MD5:	3D93B61927F958F85F5D0BA91EE339CB
SHA1:	16377A37C5A3C454DD6DA94DDB763FDA9581AC2C
SHA-256:	16E21766D86FA7336EB8854764AC9634330A2AE69088CE589291FCEE00DACA2F
SHA-512:	53EFA7724692339EE0A2A946021874463A17FA2DC9DDF84B3EC46BBEDA98C97F56E5F4B269AABD866AC002F5EACFD844B0C68114F1A60923BF9770B84426A04F
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.=.1.3.2.6.5.3.8.9.0.7.0.1.6.4.0.0.6.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.9.0.7.8.9.6.0.8.7.5.3.....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.=.5.0.4.5.f.b.7.a.-.7.e.3.d.-.4.f.b.1.-.9.b.f.b.-.a.6.7.0.2.d.f.9.e.6.3.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.1.9.5.4.d.a.-.1.0.3.d.-.4.d.e.6.-.b.c.7.4.-.e.1.0.b.d.3.8.b.7.c.6.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.0.4.a.4.-.0.0.0.1.-.0.0.1.6.-.9.8.b.0.-.d.7.a.f.0.2.4.8.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\WER4F0E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:17:53 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	53222
Entropy (8bit):	2.0234823838500255
Encrypted:	false
SSDEEP:	192:7NKKSccy8ti5JmSTJCPdFZTDpKp4qKz+PGQX//f9i4tkfNnx:xK7ccy8tiDm2CPdFZ3pW42Gi1i4t+Nx
MD5:	BD157BF0A2B31D7189E3EB22CA904C5D
SHA1:	4B9A7CE792E67C7D8806C17E8011D527EEBE6E8F
SHA-256:	6E5D359DD56BCB5B147C4FE2296C73691D154DFD2068C76D61EAB21123F1C9A9
SHA-512:	C3F30B65B1670093A9CBEFF6F3C5BF73CABFF46F524841C8D613DA9A81176E904D69B2E1603E67679C7ED1DD5ACEB5A58E447D5D5EE556E3CF6ED8EE3B11B69
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	
Preview:	MDMP..... .....5.`.....U.....B.....GenuineIntelW.....T.....4.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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):	8292
Entropy (8bit):	3.6941918391120394
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi1j6z6Yyq6SSgmfTDVSUCprm89bBnEsfkrm:RrlsNiB6z6YH6SSgmfTpSjBn3fV
MD5:	BB069A3CE0BECCE04DA1DFD5B5EE2D93
SHA1:	FBDA704404B9B69B03FE4FA0544EB1DD5DFCE45A
SHA-256:	64D662366E6B3E242E42526490EE43D33675B1F7E70DFDA9FF4A621F509A1358
SHA-512:	6B211D18EACD3B0DB46B84E920BC31B5F7B9EE31C5F7453EC990F671EDB449068E6B9DE4C61236DB8E854733E8278D4472D0BACA06576E68118BD938E595CE5
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.1.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.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):	4.469981201224701
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYJgtWI9M6WSC8B88fm8M4JCdsrNrFGX+q8/ONF54SrSsad:uITfe37SNrJ9NkXNNbDWPd
MD5:	C0B9B614D9A07EBED15EF89B7D00B184
SHA1:	DCB03D004BF473334DB24C261F700303AA06DECD
SHA-256:	C7FEB0876F463A81386FB0FD53590E9ECB11E89BB66B09413C02304D27272F84
SHA-512:	0569BCE8DCC439D9B2037799006E07BBFB513A1167ED4FFBD48166087C1FB2280AA5380DEFCC617BFCBB97D7A18F7F66FC7F9ACD76E564F676654E53416E760
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="987808" />.. <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):	7.513894160845713
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:	cdc733ac_by_Libranalysis.dll
File size:	167424
MD5:	cdc733ac9b6d09b3988e7bca1d238067
SHA1:	197fd7c03f39db96597bb3dfc46c5f10db941291

General

SHA256:	31852f33db8ce7ac6d3ffea2d05a900316a42903edaffbb8414a3f09bd62d752
SHA512:	8da39a51e7f3243e3bf64ce7939435d1509c9ad70770da79e5d8f91c91fde67e7e85508866786dccb85b75be91d14f49b5987ca98bb6043935966732542614e7
SSDEEP:	3072:S9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:S9F6rQXvFczvYpQP
File Content Preview:	MZ.....@.....\.....!..L.!This program cannot be run in DOS mode....$.....Xm.o...<...<...<.U!<...<..B<r..<...<...<rQ!<...<;..<...<;..<3..<au.<...<szt<"..<Rich...<.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10024cc0
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:	0x609C7F6E [Thu May 13 01:22:54 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:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
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
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx
mov dword ptr [10029730h], eax
mov eax, esi
mov dword ptr [10029728h], eax
jne 00007F7A84A87AF6h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Instruction
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] VS2015 build 23026 • [IMP] VS2013 UPD4 build 31101 • [C] VS2010 build 30319 • [RES] VS2015 UPD2 build 23918 • [C++] VS2005 build 50727 • [IMP] VS2010 SP1 build 40219 • [RES] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	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	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.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	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x3d61	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x957	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	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	0x2c060	0x33c	data		

Imports

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

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 07:17:11.023500919 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:11.090707064 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 07:17:11.128060102 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:11.185295105 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 07:17:11.202760935 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:11.254357100 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 07:17:11.304088116 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:11.353168011 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 07:17:11.836694002 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:11.907391071 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 07:17:13.974787951 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:14.032154083 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 07:17:14.749022007 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:14.799983025 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 07:17:15.666651011 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:15.715529919 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 07:17:16.591387987 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:16.642918110 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 07:17:18.104734898 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:18.158260107 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 07:17:18.938004017 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:18.986681938 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 07:17:20.127214909 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:20.175981045 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 07:17:20.428441048 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:20.489871979 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 07:17:21.007406950 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:21.075365067 CEST	53	63183	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:17:22.383239031 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:22.448023081 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 07:17:26.098551035 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:26.147257090 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 07:17:27.200968981 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:27.252579927 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 07:17:35.473531961 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:35.530662060 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 07:17:57.458743095 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 07:17:57.518450022 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 07:18:00.475873947 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 07:18:00.527446032 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 07:18:05.991997957 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 07:18:06.040785074 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 07:18:06.923700094 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 07:18:06.983721972 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 07:18:39.209810972 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 07:18:39.268542051 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 07:18:47.451965094 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 07:18:47.509162903 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 07:19:03.338954926 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:03.399909973 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 07:19:14.517409086 CEST	50394	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:14.574697018 CEST	53	50394	8.8.8.8	192.168.2.5
May 13, 2021 07:19:16.399549007 CEST	58530	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:16.472240925 CEST	53	58530	8.8.8.8	192.168.2.5
May 13, 2021 07:19:53.436558008 CEST	53813	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:53.548871040 CEST	53	53813	8.8.8.8	192.168.2.5
May 13, 2021 07:19:54.272459984 CEST	63732	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:54.379307985 CEST	53	63732	8.8.8.8	192.168.2.5
May 13, 2021 07:19:55.050069094 CEST	57344	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:55.107983112 CEST	53	57344	8.8.8.8	192.168.2.5
May 13, 2021 07:19:55.598221064 CEST	54450	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:55.655179024 CEST	53	54450	8.8.8.8	192.168.2.5
May 13, 2021 07:19:56.309092045 CEST	59261	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:56.366317987 CEST	53	59261	8.8.8.8	192.168.2.5
May 13, 2021 07:19:57.116682053 CEST	57151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:57.174541950 CEST	53	57151	8.8.8.8	192.168.2.5
May 13, 2021 07:19:57.670428038 CEST	59413	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:57.727732897 CEST	53	59413	8.8.8.8	192.168.2.5
May 13, 2021 07:19:58.544308901 CEST	60516	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:58.601311922 CEST	53	60516	8.8.8.8	192.168.2.5
May 13, 2021 07:19:59.572215080 CEST	51649	53	192.168.2.5	8.8.8.8
May 13, 2021 07:19:59.631011963 CEST	53	51649	8.8.8.8	192.168.2.5
May 13, 2021 07:20:00.197818041 CEST	65086	53	192.168.2.5	8.8.8.8
May 13, 2021 07:20:00.257627010 CEST	53	65086	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 3336 Parent PID: 5632

General

Start time:	07:17:20
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\cdc733ac_by_Libranalysis.dll'
Imagebase:	0x30000
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: 2964 Parent PID: 3336

General

Start time:	07:17:20
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\cdc733ac_by_Libranalysis.dll',#1
Imagebase:	0x150000
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: 1188 Parent PID: 2964

General

Start time:	07:17:20
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\cdc733ac_by_Libranalysis.dll',#1
Imagebase:	0xb10000
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: 00000002.00000002.325845384.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6204 Parent PID: 1188

General

Start time:	07:17:48
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1188 -s 768
Imagebase:	0xf70000
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	6D991717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D98497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.tmp	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	success or wait	1	6D984BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	success or wait	1	6D984BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.tmp.xml	success or wait	1	6D984BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E8F.tmp.csv	success or wait	1	6D984BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER61EC.tmp.txt	success or wait	1	6D984BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 11 35 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....5.`.....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.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 d8 1f 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 a4 04 00 00 f0 34 9d 60 07 00 00 00 11 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....4.`.................. ....0..=.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.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 ca 30 00 10 90 68 47 03 ff ff ff ff ca 30 00 10 19 06 00 02 54 f9 f1 02 ca 30 00 10 23 00 00 00 03 02 01 00 d0 f8 f1 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........0...hG......0...... T....0..#...........+.........	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	168	ac 15 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ac 25 00 00	........................0.... ....%..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	20	11 00 00 00 ec f9 42 03 00 00 00 00 14 06 00 00 bc 34 00 00	......B..........4..	success or wait	17	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	1556	bc b1 a2 77 d6 c9 a0 77 64 02 00 00 aa aa aa aa 10 00 00 00 80 fa 42 03 4c fb 42 03 aa aa aa aa 40 c7 a0 77 40 c7 a0 77 aa aa aa aa 00 30 04 03 00 30 04 03 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 30 04 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 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 aa aa aa aa 48 0f 48 03 00 00 00 00 00 00 00 00 d0 08 47 03 00 70 03 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 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 72 03 03 08 f7 3a 03 68 07 47 03 10 f7 3a 03 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wd.............B.L.B... ..@..w@..w.....0...0......d... ....d........0................ ....H.H... ....G..p................. ....Tr.... :.h.G...:.....................	success or wait	16	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	4096	98 fb 42 03 00 00 43 03 00 40 42 03 00 00 00 00 00 1e 00 00 00 00 00 00 00 30 04 03 00 00 00 00 a4 04 00 00 cc 16 00 00 00 00 00 00 00 00 00 00 00 70 03 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 9b 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..B...C..@B.............0.... ....p.......... ....p.w.............	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa ca 30 00 10 00 00 00 00 68 ea f1 02 bc 9a a2 77 23 00 00 00 06 02 00 00 d8 e8 f1 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+....................0...... h......w#...........+.........	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	48	cc 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 04 03 00 00 00 00 ec f9 42 03 00 00 00 00 14 06 00 00 bc 34 00 00 cc 02 00 00 dc 30 00 00	....0........B... ....4.......0..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.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	51	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	752	00 00 05 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 92 25 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 70 48 02 00 00 00 00 00 e0 b4 02 00 00 00 00 7e 45 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 c4 f3 00 00 00 00 00 00 61 3d 03 00 00 00 00 00 df 6b 02 00 00 00 00 00 2c 3f 1b 00 00 00 00 00 14 c0 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 de c7 21 00 00 00 00	...t.....0...U..s@...%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....pH..... ~E.....a= .....k.....,?..... @.....!....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.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 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	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F0E.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 a8 33 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 ce b1 00 00 15 00 00 00 ec 01 00 00 54 1d 00 00 16 00 00 00 98 00 00 00 40 1f 00 00	....3.....T.....8..... ....T.....`..... ..T.....@...	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 31 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.1.8.8.<./.P.i.d.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 37 00 32 00 33 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.>.3.2.7.2.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 37 00 38 00 32 00 33 00 38 00 37 00 32 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.>.1.2.7.8.2.3.8.7.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 37 00 38 00 31 00 35 00 36 00 38 00 30 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.>.1.2.7.8.1.5.6.8.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 32 00 33 00 36 00 34 00 38 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.>.9.2.3.6.4.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 32 00 33 00 36 00 34 00 38 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.>.9.2.3.6.4.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 34 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.>.1.8.4.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 37 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.7.1.2.<./.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.4.4.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.1.4.6.2.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 32 00 32 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.2.2.8.1.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.9.1.4.6.2.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.9.6.4.<./.P.i.d.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 33 00 31 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.1.0.7. <./.U.p.t.i.m.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 33 00 30 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.>.1.1.3.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 35 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.5.5.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 36 00 39 00 38 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.8.6.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 31 00 36 00 37 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.>.3.6.1.6.7.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 79 00 65 00 75 00 76 00 69 00 6f 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.y.e.u.v.i.o.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 79 00 65 00 75 00 76 00 69 00 6f 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.y.e.u.v.i.o.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 38 00 32 00 32 00 33 00 38 00 30 00 39 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.8.2.2.3.8.0.9.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 31 00 34 00 3a 00 31 00 37 00 3a 00 35 00 33 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.1.4.:.1.7.:.5.3.Z.".>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 31 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 36 00 30 00 36 00 32 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 36 00 30 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.4.". .P.I.D.=.".1.1.8.8.". .U.p.t.i.m.e.M.S.=.".2.6.0.6.2.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.6.0.6.2.". .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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 30 00 34 00 35 00 66 00 62 00 37 00 61 00 2d 00 37 00 65 00 33 00 64 00 2d 00 34 00 66 00 62 00 31 00 2d 00 39 00 62 00 66 00 62 00 2d 00 61 00 36 00 37 00 30 00 32 00 64 00 66 00 39 00 65 00 36 00 33 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.5.0.4.5.f.b.7.a.-.7.e.3.d.-.4.f.b.1.-.9.b.f.b.-.a.6.7.0.2.d.f.9.e.6.3.9.<./.G.u.i.d.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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 31 00 34 00 3a 00 31 00 37 00 3a 00 35 00 33 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.1.4.:.1.7.:.5.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF0.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	6D98497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E82.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	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718\Report.wer	unknown	2	ff fe	..	success or wait	1	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718\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	182	6D98497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1b9fa90771cb5b9a349a2796affd510a5b149_82810a17_18727718\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 39 00 39 00 36 00 34 00 35 00 34 00 38 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.1.9.9.6.4.5.4.8.4.	success or wait	1	6D98497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D9A36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D9A1FB2	RegCreateKeyExW
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9843D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D9A36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D9A36BF	unknown
\REGISTRY\A\{5aa88dac-8e67-85ee-88f4-9f40f21aef56}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D9A36BF	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 CA 30 00 10 02 00 00 00 01 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D9A1FE8	RegSetValueExW

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

Disassembly

Code Analysis