ID: 413044
Sample Name:
052a78c5_by_Libranalysis.dll
Cookbook: default.jbs
Time: 07:01:54
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

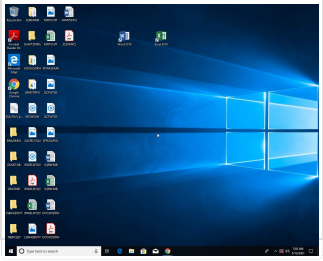
Analysis Report 052a78c5_by_Libranalysis.dll

Overview

General Information

Sample Name:	052a78c5_by_Libranalysis.dll
Analysis ID:	413044
MD5:	052a78c50ecacc…
SHA1:	47b557ff30577de..
SHA256:	457e30cbead2eb..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

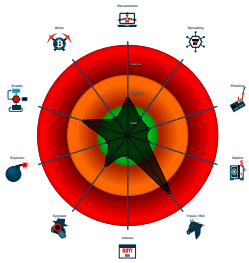
Dridex

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 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: 6868 cmdline: loaddll32.exe 'C:\Users\user\Desktop\052a78c5_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6880 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\052a78c5_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6892 cmdline: rundll32.exe 'C:\Users\user\Desktop\052a78c5_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6724 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6892 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvpltFNCpvA5goSylkxjIBtIwWPTv1DPbNEcuIekQC7O"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.751164922.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

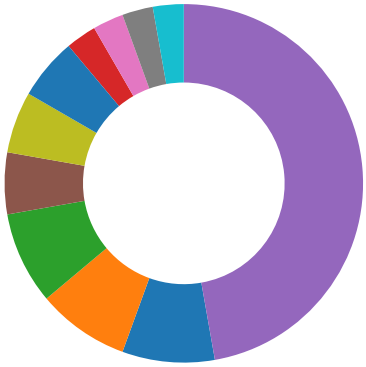
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

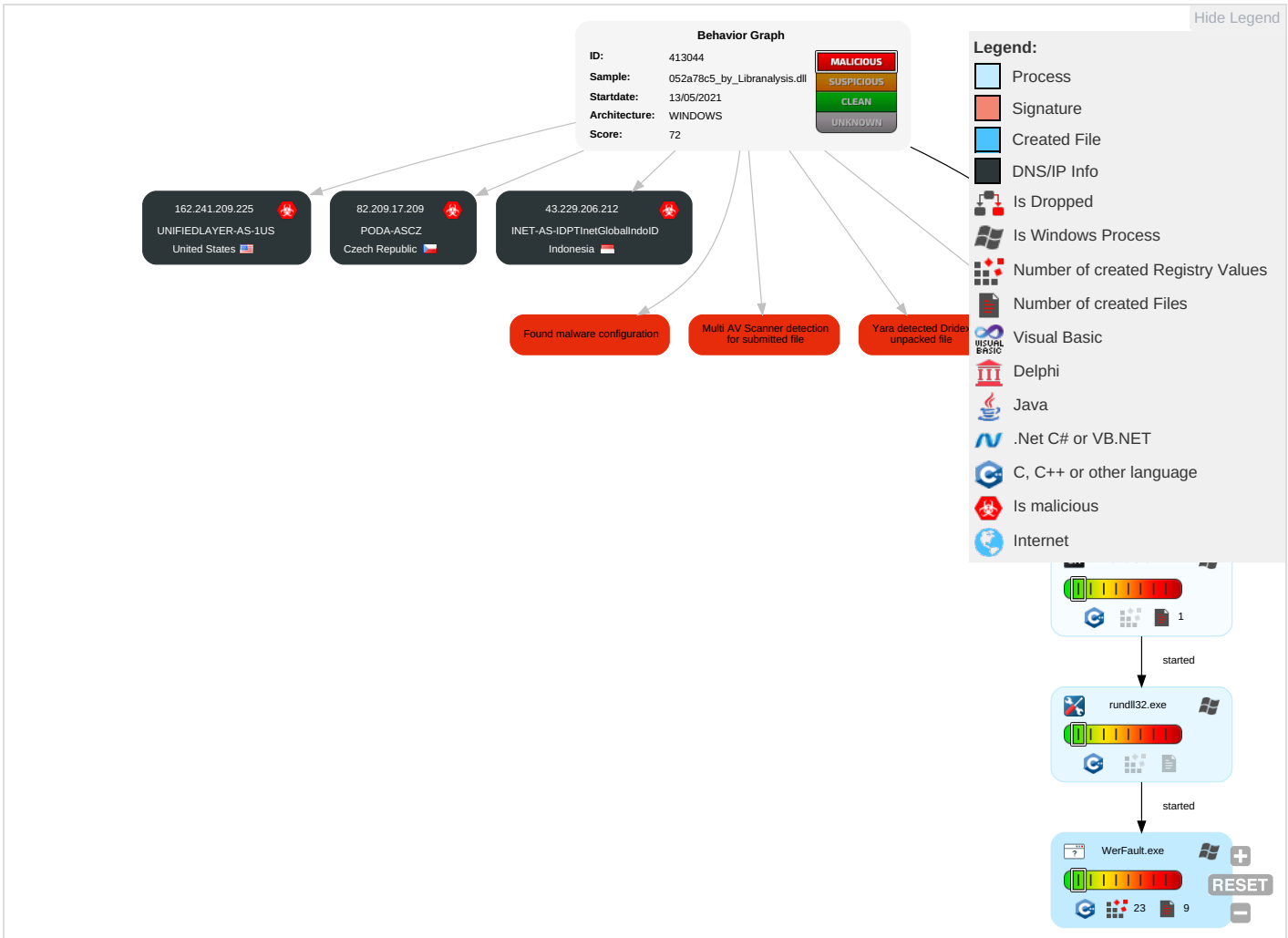
Yara detected Dridex unpacked file

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	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on 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	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Security Account Manager	Account Discovery 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)	Process Injection 1 1	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 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

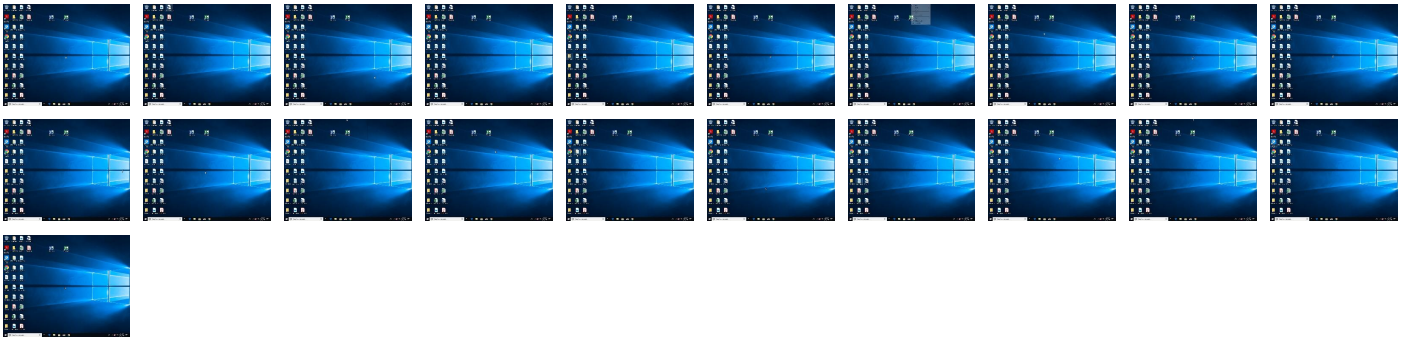
Behavior Graph



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
052a78c5_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
052a78c5_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.760000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

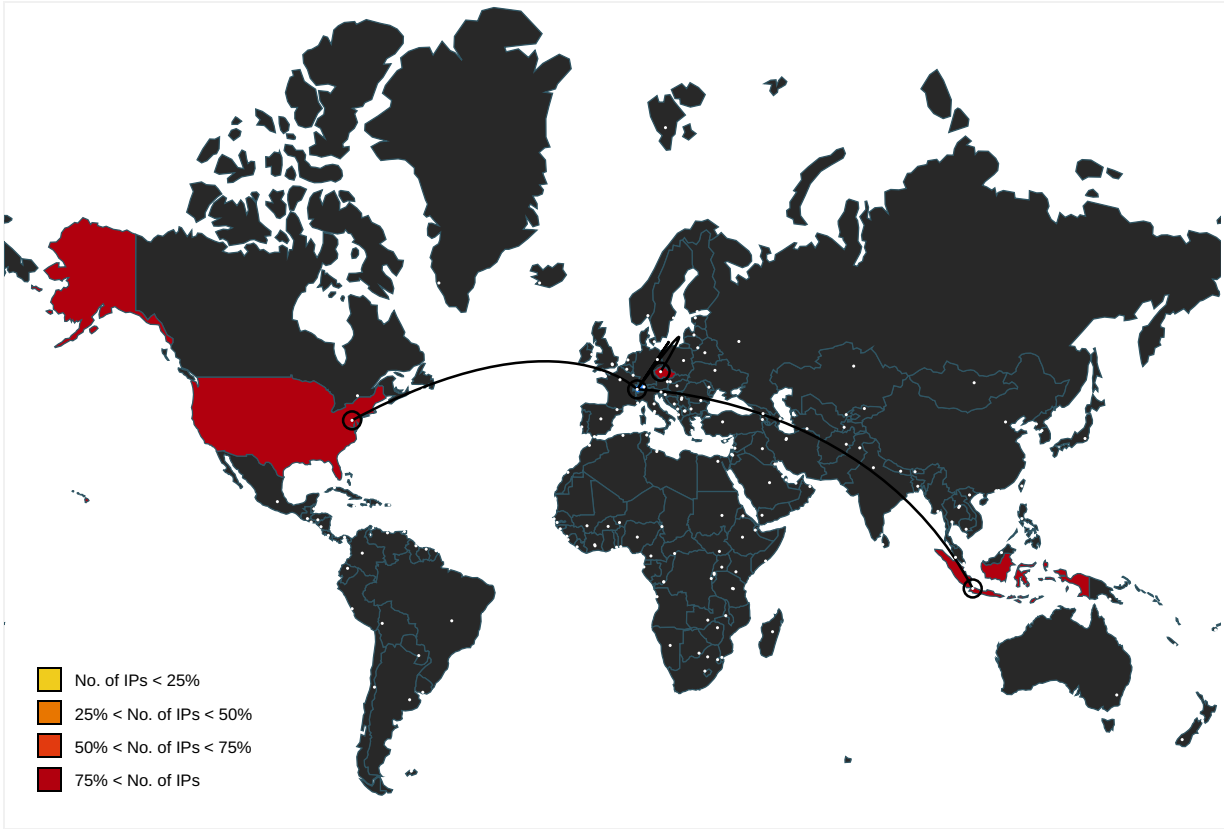
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

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:	413044
Start date:	13.05.2021

Start time:	07:01:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	052a78c5_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:	20
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: 94.4% (good quality ratio 86.6%) • Quality average: 72.2% • Quality standard deviation: 32%
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 • Stop behavior analysis, all processes terminated

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	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	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	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	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	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	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
UNIFIEDLAYER-AS-1US	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	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
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12480
Entropy (8bit):	3.768003396208444
Encrypted:	false
SSDEEP:	192:z5isQ0oXfecHBUZMX4jed+oG/u7saS274ItWc2:NilXdBUZMX4jek/u7saX4ItWc2
MD5:	C79C46CAEBE4428EFA5921130A539BA1
SHA1:	F093D15AD17F02CF2570DDBFEEB5FB8F96FEE682
SHA-256:	1032F66F4CCF90FAD2A596E6D1DECF216E03A5BF54F33146055BC926928C8414
SHA-512:	965089DB9348522AA045D59300B57612CA37A9292C6ACA2437CAF28C3049CCB34A04669AE3F0E5F91F8C873CB9A53241370D6C60EEB1D5D612129482F37ED83D
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.5.5.7.9.9.2.2.3.5.8.1.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.5.5.8.0.6.7.2.3.5.5.5.8.....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.=.1.e.6.0.0.c.0.e.-.e.2.c.8.-.4.c.2.5.-.b.e.6.d.-.e.4.c.0.9.7.3.1.9.1.7.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.2.a.6.2.9.5.9.-.6.d.9.6.-.4.5.c.c.-.a.5.8.f.-.6.7.7.d.1.c.7.b.b.2.5.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.c.-.0.0.0.1.-.0.0.1.b.-.5.4.0.6.-.7.b.3.7.b.5.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 05:03:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	53946
Entropy (8bit):	1.960471805872159
Encrypted:	false
SSDEEP:	192:PEQvUwOF+uMeS15WNtYh9Th9C4Qkk8MSpjpdPPOz3zFAwcTE3AjGbnKX+w:L7lrF56QR00p1d+FYTE39bKX+w
MD5:	372D3AD8CB267B81AE6A9CFE45885929
SHA1:	8686BACF44AD28537595A4E6A40ACAC4659F6E59
SHA-256:	CD9339379C742E8CBD076FBD24F2C39EB7C09D982AB9EDA470A8DFCE61626ECC
SHA-512:	81769D0D2C7D5DF76ED998031642815725C1D78BD2A022D11941616DF81633CE882BDF88F0C03B1BC99417E131DF7126D724A1C0C066E57433B503BC34408B9C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....`.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	3.693730370144414
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioS6086Yda6ZVgmfTtVSp+pru89bBosfxLm:RrlsNil6n6Yw6ZVgmfT3SKBbfA
MD5:	0D8AA58C0E30E6C5C2246F459A566B10
SHA1:	328A5F5F4E41238A04BC08BFDDC8AC8A51B00FFD
SHA-256:	652B199B5E258331FBC17BA3EFFC8F92FE06A2A12FFA7CFDAED4839ABC97FA8A
SHA-512:	4039DD541A9F3CCE88477B6BBF78F36A9BD582AB3022DB13B71B4471596447335BF8C7DC8597AB482C8740736A00026B0EC08EF2488A46757006C6BECA1E9609
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.tmp.xml	
Entropy (8bit):	4.474049710089997
Encrypted:	false
SSDEEP:	48:cvIwSD8zsy+JgtWI9ScWSC8B78fm8M4JCds5NrFUC+q8/QNFN4SrSid:uITfNVVSNOJHNeC3NHDWid
MD5:	435FA0B0D3FDB437A77945DFCD1D585C
SHA1:	83F4F3571DA3D5D6E0831191146A279A91A6B6A8
SHA-256:	77860D0322952C8901E15FFCBF132AC92A6A0722FAFD35BBDDB1766677611EA3
SHA-512:	735A47E38596D5D34050601597DC39BD476DB29CFD8519F1F5C7DBFBC834C402256D9AAB0AAAB755C8F91DBDCC1E603FE4A1E02860A3E81070DE9B0BDFD33A51
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="987254" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513890585129229
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:	052a78c5_by_Libranalysis.dll
File size:	167424
MD5:	052a78c50ecacc62446415769e5f5630
SHA1:	47b557ff30577de5f4150cb28b42eb8640a49402
SHA256:	457e30cbead2eb1e765d115acaa0e7eaee8cf1682f0ffd2f037042f610abedc4
SHA512:	9b39a6534329ddb637336a7f84c1418e0886ddef348eda2e26ef1074b806ff4d1417e3a76b1e3339224f55b28bc241735deec2824deeaa87723471ef4988696c
SSDEEP:	3072:W9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:W9F6rQXvFczvYpQP
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:	0x609C8123 [Thu May 13 01:30:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

General

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 00007F2340D9A496h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

Programming Language:	[RES] 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

Name	Virtual Address	Virtual Size	Is in Section
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	0x38ee	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x6c9	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

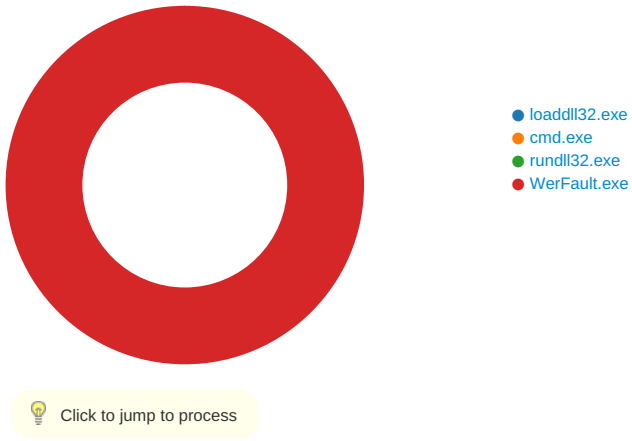
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:02:40.298676014 CEST	54531	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:40.347475052 CEST	53	54531	8.8.8.8	192.168.2.4
May 13, 2021 07:02:42.264461040 CEST	49714	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:42.316142082 CEST	53	49714	8.8.8.8	192.168.2.4
May 13, 2021 07:02:43.987989902 CEST	58028	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:44.046974897 CEST	53	58028	8.8.8.8	192.168.2.4
May 13, 2021 07:02:47.515320063 CEST	53097	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:47.564148903 CEST	53	53097	8.8.8.8	192.168.2.4
May 13, 2021 07:02:48.783612967 CEST	49257	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:48.832529068 CEST	53	49257	8.8.8.8	192.168.2.4
May 13, 2021 07:02:49.905334949 CEST	62389	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:49.958391905 CEST	53	62389	8.8.8.8	192.168.2.4
May 13, 2021 07:02:51.382716894 CEST	49910	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:51.434392929 CEST	53	49910	8.8.8.8	192.168.2.4
May 13, 2021 07:02:52.705286026 CEST	55854	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:52.756772995 CEST	53	55854	8.8.8.8	192.168.2.4
May 13, 2021 07:02:53.811158895 CEST	64549	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:53.862827063 CEST	53	64549	8.8.8.8	192.168.2.4
May 13, 2021 07:02:55.075272083 CEST	63153	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:55.124031067 CEST	53	63153	8.8.8.8	192.168.2.4
May 13, 2021 07:02:56.353646994 CEST	52991	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:56.409771919 CEST	53	52991	8.8.8.8	192.168.2.4
May 13, 2021 07:02:58.451255083 CEST	53700	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:58.500503063 CEST	53	53700	8.8.8.8	192.168.2.4
May 13, 2021 07:02:59.723622084 CEST	51726	53	192.168.2.4	8.8.8.8
May 13, 2021 07:02:59.772427082 CEST	53	51726	8.8.8.8	192.168.2.4
May 13, 2021 07:03:01.118149042 CEST	56794	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:01.191689968 CEST	53	56794	8.8.8.8	192.168.2.4
May 13, 2021 07:03:06.071620941 CEST	56534	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:06.133546114 CEST	53	56534	8.8.8.8	192.168.2.4
May 13, 2021 07:03:07.304764032 CEST	56627	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:07.353646994 CEST	53	56627	8.8.8.8	192.168.2.4
May 13, 2021 07:03:08.658782959 CEST	56621	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:08.707977057 CEST	53	56621	8.8.8.8	192.168.2.4
May 13, 2021 07:03:10.109338999 CEST	63116	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:10.160792112 CEST	53	63116	8.8.8.8	192.168.2.4
May 13, 2021 07:03:11.284595966 CEST	64078	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:11.334393978 CEST	53	64078	8.8.8.8	192.168.2.4
May 13, 2021 07:03:14.225765944 CEST	64801	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:14.274611950 CEST	53	64801	8.8.8.8	192.168.2.4
May 13, 2021 07:03:15.072634935 CEST	61721	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:15.139296055 CEST	53	61721	8.8.8.8	192.168.2.4
May 13, 2021 07:03:27.774710894 CEST	51255	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:27.823393106 CEST	53	51255	8.8.8.8	192.168.2.4
May 13, 2021 07:03:36.517241001 CEST	61522	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:36.577717066 CEST	53	61522	8.8.8.8	192.168.2.4
May 13, 2021 07:03:40.964303017 CEST	52337	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:41.016127110 CEST	53	52337	8.8.8.8	192.168.2.4
May 13, 2021 07:03:42.679987907 CEST	55046	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:42.740180016 CEST	53	55046	8.8.8.8	192.168.2.4
May 13, 2021 07:03:43.370191097 CEST	49612	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:43.419434071 CEST	53	49612	8.8.8.8	192.168.2.4
May 13, 2021 07:03:43.826210022 CEST	49285	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:43.883106947 CEST	53	49285	8.8.8.8	192.168.2.4
May 13, 2021 07:03:44.681723118 CEST	50601	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:44.741580009 CEST	53	50601	8.8.8.8	192.168.2.4
May 13, 2021 07:03:44.764508963 CEST	60875	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:44.829205990 CEST	53	60875	8.8.8.8	192.168.2.4
May 13, 2021 07:03:45.512326002 CEST	56448	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:03:45.569622040 CEST	53	56448	8.8.8.8	192.168.2.4
May 13, 2021 07:03:46.035665035 CEST	59172	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:46.095222950 CEST	53	59172	8.8.8.8	192.168.2.4
May 13, 2021 07:03:46.856430054 CEST	62420	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:46.913651943 CEST	53	62420	8.8.8.8	192.168.2.4
May 13, 2021 07:03:47.891093016 CEST	60579	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:47.948112965 CEST	53	60579	8.8.8.8	192.168.2.4
May 13, 2021 07:03:48.418500900 CEST	50183	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:48.475902081 CEST	53	50183	8.8.8.8	192.168.2.4
May 13, 2021 07:03:55.048518896 CEST	61531	53	192.168.2.4	8.8.8.8
May 13, 2021 07:03:55.107655048 CEST	53	61531	8.8.8.8	192.168.2.4
May 13, 2021 07:04:24.020845890 CEST	49228	53	192.168.2.4	8.8.8.8
May 13, 2021 07:04:24.093415976 CEST	53	49228	8.8.8.8	192.168.2.4
May 13, 2021 07:04:26.129225969 CEST	59794	53	192.168.2.4	8.8.8.8
May 13, 2021 07:04:26.186403990 CEST	53	59794	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6868 Parent PID: 5916

General

Start time:	07:02:47
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\052a78c5_by_Libranalysis.dll'
Imagebase:	0x9a0000
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: 6880 Parent PID: 6868

General

Start time:	07:02:47
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\052a78c5_by_Libranalysis.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6892 Parent PID: 6880

General

Start time:	07:02:47
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\052a78c5_by_Libranalysis.dll',#1
Imagebase:	0x1220000
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: 00000002.00000002.751164922.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6724 Parent PID: 6892

General

Start time:	07:03:17
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6892 -s 764
Imagebase:	0x320000
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	6F591717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F58497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.tmp	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	success or wait	1	6F584BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	success or wait	1	6F584BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.tmp.xml	success or wait	1	6F584BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F82.tmp.csv	success or wait	1	6F584BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER981E.tmp.txt	success or wait	1	6F584BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 18 b3 9c 60 a4 05 12 00 00 00 00 00	MDMP..... .....`.....	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.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 ec 1a 00 00 f7 b2 9c 60 08 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 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....`.................. ....0..=...............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.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 20 35 5f 00 ff ff ff ff ca 30 00 10 19 06 00 02 2c fe 16 00 ca 30 00 10 23 00 00 00 03 02 01 00 a8 fd 16 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........0.. 5_......0...... ,....0..#...........+.........	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	168	f0 1a 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 00 00 00 cc 02 00 00 ac 25 00 00	........................0.... ....%..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	20	12 00 00 00 c0 f6 59 00 00 00 00 00 40 09 00 00 cc 34 00 00	......Y.....@....4..	success or wait	18	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	2368	bc b1 11 77 d6 c9 0f 77 64 02 00 00 aa aa aa aa 10 00 00 00 54 f7 59 00 20 f8 59 00 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 60 33 00 00 60 33 00 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 60 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 bd 5e 00 00 00 00 00 00 00 00 00 b0 08 5f 00 00 00 33 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 18 f9 71 00 54 02 33 00 20 f9 71 00 48 07 5f 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wd...........T.Y. .Y... ..@..w@..w.....`3..`3.....d... ....d........`3.............. ............................. ........................`.^... ...._...3................ ....q.T.3. .q.H._....................	success or wait	17	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	1972	bc b1 11 77 d6 c9 0f 77 64 02 00 00 aa aa aa aa 10 00 00 00 e0 f8 71 00 ac f9 71 00 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 90 33 00 00 90 33 00 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 90 33 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 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 58 06 5f 00 00 00 00 00 00 00 00 00 b0 08 5f 00 00 00 33 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa f0 f7 b5 00 8c f7 59 00 f8 f7 b5 00 94 f7 59 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	...w...wd............q...q... ..@..w@..w......3...3.....d... ....d.........3.............. ....X._... ...._...3................ .... Y.......Y....................	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.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 40 ef 16 00 bc 9a 11 77 23 00 00 00 12 02 00 00 b0 ed 16 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+....................0...... @......w#...........+.........	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	48	fc 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 c0 33 00 00 00 00 00 24 f7 b5 00 00 00 00 00 dc 08 00 00 20 3e 00 00 cc 02 00 00 dc 30 00 00	....3.....$........... >.......0..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	752	00 00 74 73 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 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 f0 a8 02 00 00 00 00 00 50 23 03 00 00 00 00 88 62 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 97 79 03 00 00 00 00 00 af 79 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a7 e1 1a 00 00 00 00 00 99 1d 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 ed 30 05 00 00 00 00	..ts.....0...U..s@...%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....P#..... .b.....y.....y ..... @.....0.....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8541.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 24 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 a2 b4 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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.9.2.<./.P.i.d.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 34 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.4.0.2.<./.U.p.t.i.m.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 34 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.>.2.7.0.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 38 00 33 00 32 00 33 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.>.9.1.8.3.2.3.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 38 00 33 00 32 00 33 00 32 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.>.9.1.8.3.2.3.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.0.4.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.7.6.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 30 00 30 00 30 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.9.0.0.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 38 00 39 00 38 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.9.8.2.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 30 00 30 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.9.0.0.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.8.0.<./.P.i.d.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 37 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.7.9.0.<./.U.p.t.i.m.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 37 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.>.1.1.1.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 39 00 31 00 36 00 38 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.>.3.7.1.9.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 34 00 37 00 33 00 34 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.4.7.3.4.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 38 00 33 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.1.8.3.3.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 35 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.7.1.7.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 31 00 38 00 33 00 33 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.1.8.3.3.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 64 00 64 00 73 00 74 00 62 00 62 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.>.d.d.s.t.b.b.,. .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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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 64 00 64 00 73 00 74 00 62 00 62 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.>.d.d.s.t.b.b.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 35 00 36 00 35 00 31 00 35 00 31 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.5.6.5.1.5.1.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 30 00 35 00 3a 00 30 00 33 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.0.5.:.0.3.:.2.1.Z.".>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 37 00 39 00 36 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 38 00 37 00 39 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.8.". .P.I.D.=.".6.8.9.2.". .U.p.t.i.m.e.M.S.=.".2.8.7.9.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.8.7.9.6.". .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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 65 00 36 00 30 00 30 00 63 00 30 00 65 00 2d 00 65 00 32 00 63 00 38 00 2d 00 34 00 63 00 32 00 35 00 2d 00 62 00 65 00 36 00 64 00 2d 00 65 00 34 00 63 00 30 00 39 00 37 00 33 00 31 00 39 00 31 00 37 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.e.6.0.0.c.0.e.-.e.2.c.8.-.4.c.2.5.-.b.e.6.d.-.e.4.c.0.9.7.3.1.9.1.7.6.<./.G.u.i.d.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 30 00 35 00 3a 00 30 00 33 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.0.5.:.0.3.:.2.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C18.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	6F58497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8F94.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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\Report.wer	unknown	2	ff fe	..	success or wait	1	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\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	6F58497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_add7eaf1c3ebbc81c9b6d96f4381e922a44a9_82810a17_1a2ba924\Report.wer	unknown	44	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 33 00 37 00 33 00 30 00 39 00 37 00 36 00 38 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.3.7.3.0.9.7.6.8.8.	success or wait	1	6F58497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6F5A36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F5A1FB2	RegCreateKeyExW
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5843D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F5A36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6F5A36BF	unknown
\REGISTRY\A\{e597ca9b-566e-c5e5-9b9b-9bff2ba49c50}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6F5A36BF	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	6F5A1FE8	RegSetValueExW

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

Disassembly

Code Analysis