ID: 413037
Sample Name:
6333f266_by_Libranalysis.dll
Cookbook: default.jbs
Time: 06:51:48
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 6333f266_by_Libranalysis.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Dridex 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
E-Banking Fraud: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 14
Data Directories 14
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15

UDP Packets 15
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: loaddll32.exe PID: 5500 Parent PID: 5940 17
General 17
File Activities 17
Analysis Process: cmd.exe PID: 6036 Parent PID: 5500 18
General 18
File Activities 18
Analysis Process: rundll32.exe PID: 5796 Parent PID: 6036 18
General 18
Analysis Process: WerFault.exe PID: 6608 Parent PID: 5796 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
Registry Activities 41
Key Created 41
Key Value Created 41
Disassembly 42
Code Analysis 42

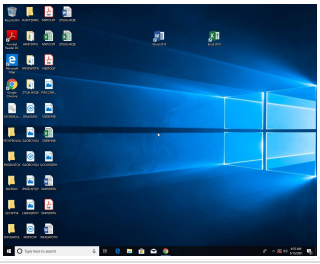
Analysis Report 6333f266_by_Libranalysis.dll

Overview

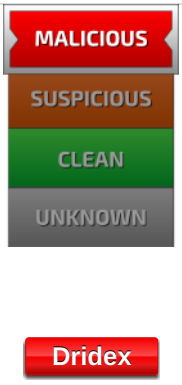
General Information

Sample Name:	6333f266_by_Libranalysis.dll
Analysis ID:	413037
MD5:	6333f266f73fb35…
SHA1:	4d686c7da1834c..
SHA256:	048a26a219a696..
Infos:	

Most interesting Screenshot:



Detection

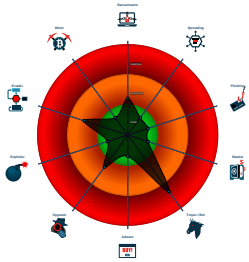


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5500 cmdline: loaddll32.exe 'C:\Users\user\Desktop\6333f266_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6036 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\6333f266_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5796 cmdline: rundll32.exe 'C:\Users\user\Desktop\6333f266_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6608 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5796 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22202,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "UlufoCqJDohDzGOdBY6ldd1IbFW5KV8BqCAnkqwdDzvq0CsZO0ngL"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.432220422.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview

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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

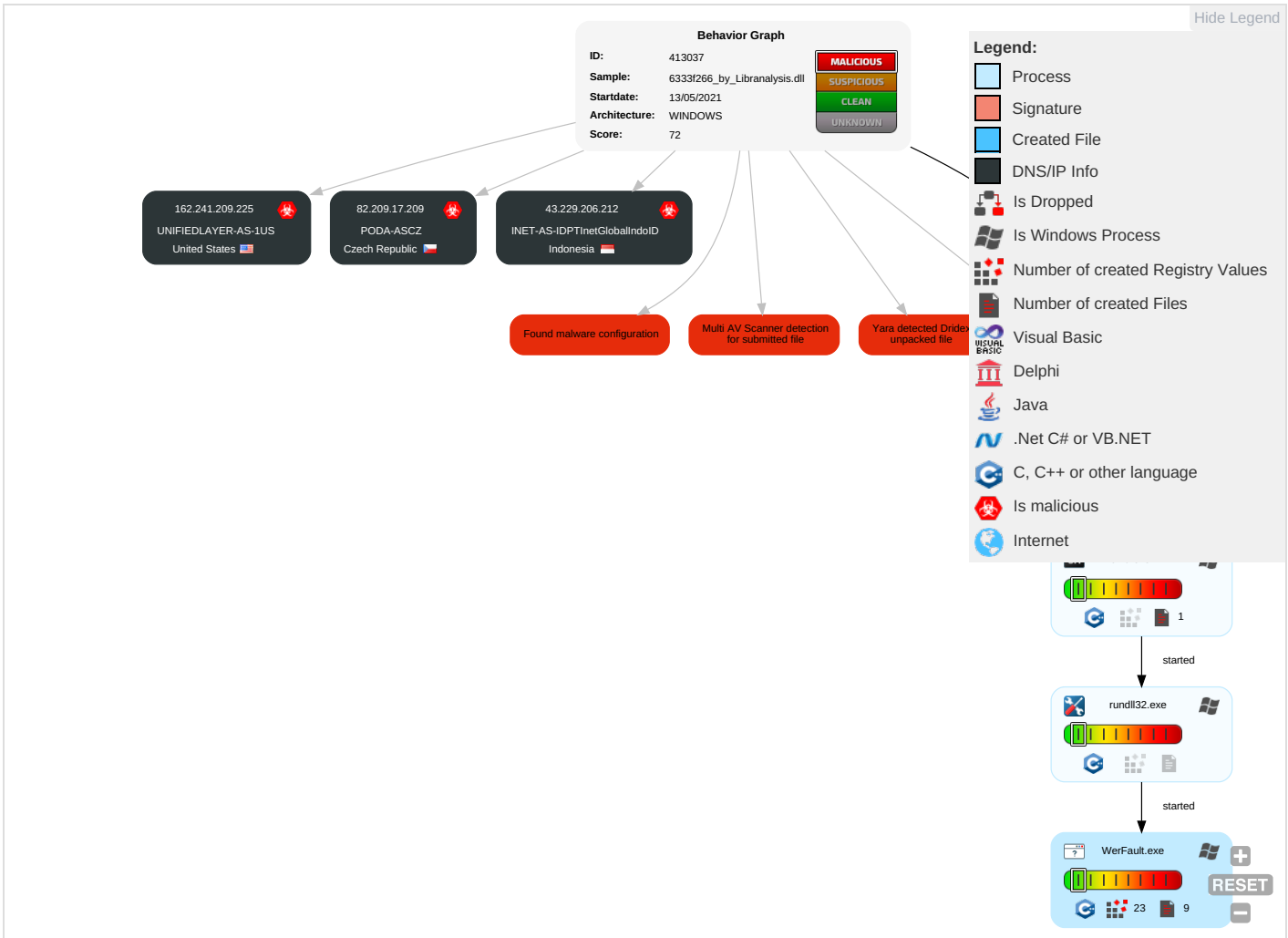
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	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)	Rundll32 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	Software Packing 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

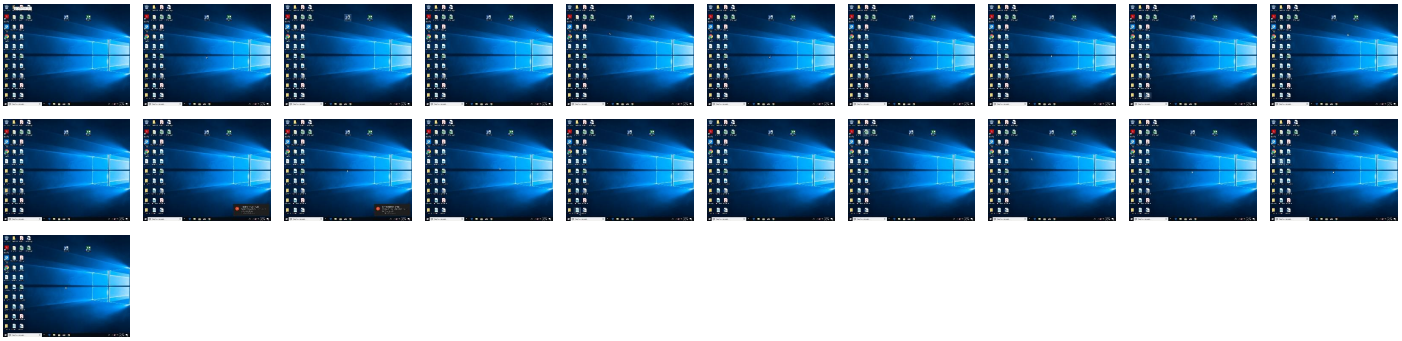
Behavior Graph



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
6333f266_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
6333f266_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.3060000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.micro0g~	0%	Avira URL Cloud	safe	

Domains and IPs

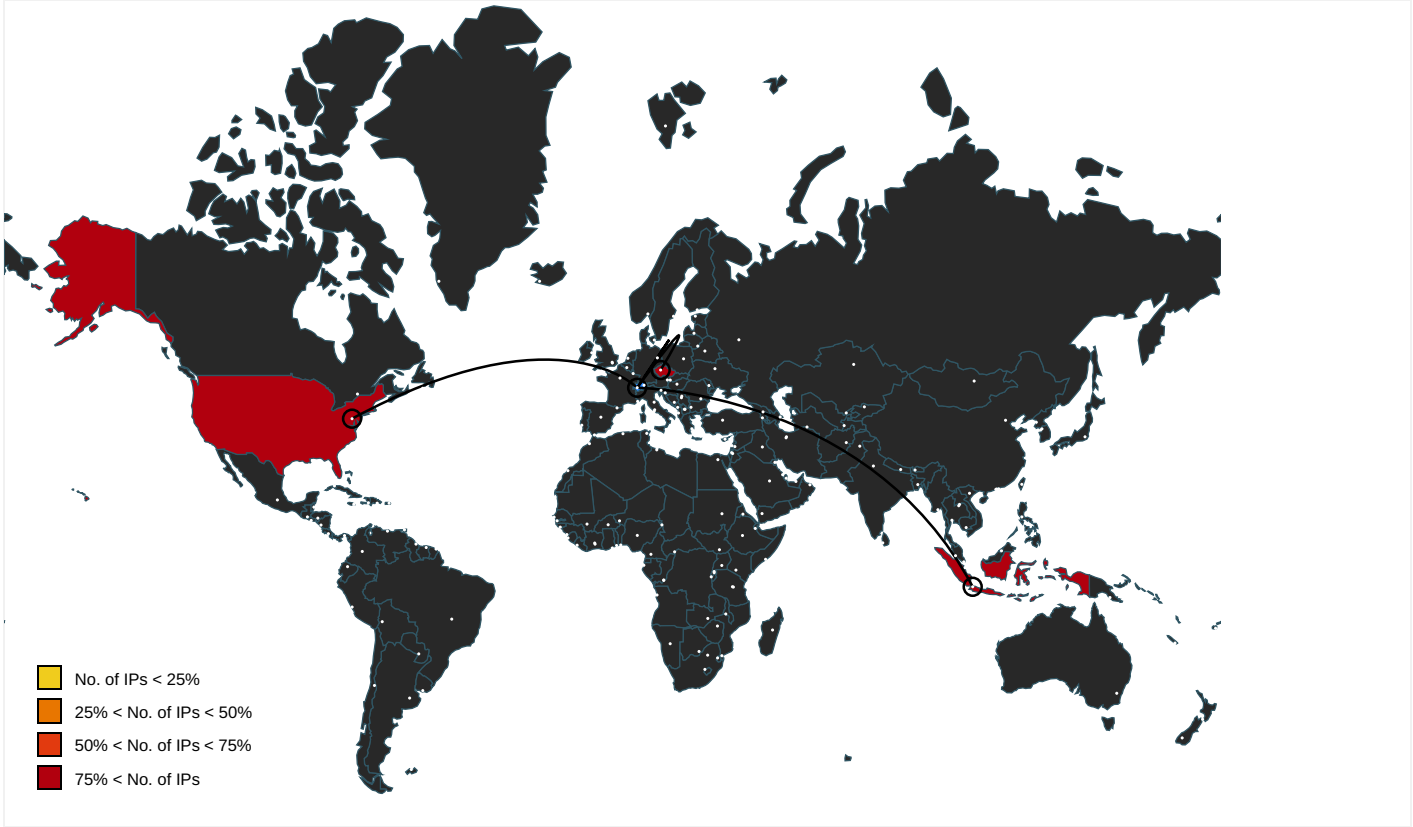
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro0g~	WerFault.exe, 00000009.0000000 3.426438405.00000000047E4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

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:	413037
Start date:	13.05.2021
Start time:	06:51:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6333f266_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:	25
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: 97.4% (good quality ratio 82%) • Quality average: 61.6% • Quality standard deviation: 36.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	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	

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

Domains

No context

ASN

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	634459e1_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_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12488
Entropy (8bit):	3.76630826150759
Encrypted:	false
SSDEEP:	192:SvViYt0oXHolSHBUZMX4jed+CG/u7saS274ltWcW:SNi+XI4BUZMX4jem/u7saX4ltWcW
MD5:	165B2317CB9EF58B27F524BBE042D7C4
SHA1:	9A2E50A3F3DEE35A18B5D0CEE3EE11B5FB8C85B4
SHA-256:	BCDD873747A3854D78A8F036FFC3CCF1A93CC3E4CD58A41E46514F5CA78DA002
SHA-512:	3A7A2160BF5D1F64DB92EFCCBD8A55ADF212BA1664CBAD97A5735535662B3B0F99E85E63B4A349D2144F9ED07F103E8DA8C059C6447E09929ADD8A2FC39FE20
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.7.5.9.5.3.6.3.3.3.3.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.7.6.0.3.0.0.3.9.2.6.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.0.2.c.2.5.c.1.-.6.1.b.5.-.4.e.3.2.-.9.c.4.6.-.8.f.7.1.e.a.f.8.3.4.b.e.....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.=.c.f.5.2.a.5.f.a.-.e.e.e.0.-.4.3.d.f.-.a.1.4.7.-.f.d.b.c.5.f.a.5.4.2.6.3.....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.=.0.0.0.0.1.6.a.4.-.0.0.0.1.-.0.0.1.7.-.7.8.d.8.-.5.9.4.0.f.f.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\WER85CF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:53:17 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	52846
Entropy (8bit):	2.0162538951164253
Encrypted:	false
SSDEEP:	192:is7746OzAtF53q4ott+XQuqLiprpW3MzEsQhPvPY/5d5nP:H7890tF53qDtt+XVqmpdWeQhvY/fZP
MD5:	34BEB8F30644634CBB39BEEDB851AB0F
SHA1:	FD6638A086DAACBE601674B2C9A9E73C99DE07FA
SHA-256:	5C7BE75A410C53B5FB95A66DA9852439162157003998 94F4797E1FC15D13CA44
SHA-512:	5D9AFD936619639B0F2CC4E8147044848FB39E35A3A6D0DD32FCA89A70A5742EF8D251392000374D948203F73064FD5FE0C874000C9889ABEFDA9A7CCE5DE03
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....M/.`.....U.....B.....GenuineIntelW.....T.....-/.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8292
Entropy (8bit):	3.697738946319232
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4B6Z6Ywg6wgmfTrLS6Cpr489bOXsfcNam:RrlsNiG6Z6Yf6wgmfTvSnOcfcx
MD5:	17F2D4D16421684BF9560639374BC47C
SHA1:	32D299A90B3E7481A840EAE5589C76B12DB39C9B
SHA-256:	E3F9BD126892B215C790A3DE36228DF9344B615875A90C4C4A64A2A6504D4212
SHA-512:	22868240A71CD546F41D9CBC1C5771C92E24DFF3EC63F06A6E74BF3F51683C6879671128D55375765807721A0C0C3A069066CE5A3B944B41C62BC286FFEA651C
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.>.5.7.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4663
Entropy (8bit):	4.479176586341754
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI992BEWSC8BR8fm8M4JCdsBNpFb/Sb+q8/0NFI4SrSFd:uITfCT/SN0JDNibTNiDWFd
MD5:	64EAA1256B041A3EFC25EFDD77EFD42A
SHA1:	5AC3CC6359B55EE216E42DC1A4EA273E156E30C5
SHA-256:	48F1BBFD13B98436AC0DB78AB844477CABFBD4422CAF568150424EA2FB700663
SHA-512:	CF08A9CBAE338670AF078DFB5889B35ADEF45F7950F57007B1143F268824DBA8F2A4013E6B0E8E6E3453AE4800132ED06A2124ADCAF31E84C2BDF301F46D767
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987783" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.510319748622296
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:	6333f266_by_Libranalysis.dll
File size:	167424
MD5:	6333f266f73fb35f0f098cefda1514d0
SHA1:	4d686c7da1834c361d0e85cb0926c1d2f44ff446
SHA256:	048a26a219a696a17a164d66928c5231f8a798c8a07340c44df4c3721eca9d60
SHA512:	4fc3d4b0fe15f5716b2c8c09c8df0db6a71de9b10ef8fc92292cfb541631a6820c5a6fdfa8c48708deebe3aea661dfcdf674ec16887ee389c0d792aa3aa61990
SSDEEP:	3072:iar6Ys6p54kfdo+APr0aYSbeO6aal8jeytFQTOpp2J:Us4p+ADxnSO6D2cOp
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:	0x10024b60
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:	0x609C7F8C [Thu May 13 01:23:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a5d8d3bddce161fe65c4f476bd18c6da

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 00007FF6E909AEA6h
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
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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x23c9e	0x23e00	False	0.753620426829	data	7.52981613282	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.749112215909	data	7.3747682631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x3c8c	0x1800	False	0.8125	MMDF mailbox	7.51564718747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0xce2	0x400	False	0.5439453125	data	4.2612921869	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
CLUSAPI.dll	ClusterEnum
USER32.dll	TranslateMessage
KERNEL32.dll	LoadLibraryW, GetProfileSectionW, GetProfileSectionA, OpenSemaphoreW, CreateFileW, OutputDebugStringA, CloseHandle
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
ADVAPI32.dll	RegOverridePredefKey
RASAPI32.dll	RasGetConnectionStatistics

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:52:36.563555002 CEST	53	58377	8.8.8.8	192.168.2.6
May 13, 2021 06:52:37.125205040 CEST	55074	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:37.174005032 CEST	53	55074	8.8.8.8	192.168.2.6

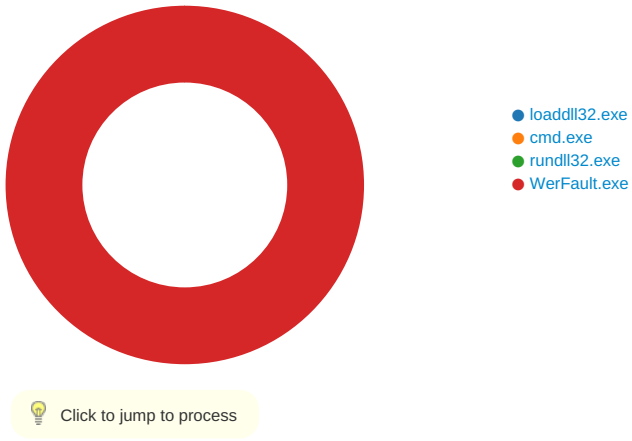
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:52:38.805898905 CEST	54513	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:38.857475042 CEST	53	54513	8.8.8.8	192.168.2.6
May 13, 2021 06:52:40.016448975 CEST	62044	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:40.067193031 CEST	53	62044	8.8.8.8	192.168.2.6
May 13, 2021 06:52:40.923135996 CEST	63791	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:40.975631952 CEST	53	63791	8.8.8.8	192.168.2.6
May 13, 2021 06:52:42.353985071 CEST	64267	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:42.411580086 CEST	53	64267	8.8.8.8	192.168.2.6
May 13, 2021 06:52:43.524728060 CEST	49448	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:43.573529959 CEST	53	49448	8.8.8.8	192.168.2.6
May 13, 2021 06:52:44.647708893 CEST	60342	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:44.698282957 CEST	53	60342	8.8.8.8	192.168.2.6
May 13, 2021 06:52:47.779062986 CEST	61346	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:47.827877045 CEST	53	61346	8.8.8.8	192.168.2.6
May 13, 2021 06:52:48.892020941 CEST	51774	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:48.949282885 CEST	53	51774	8.8.8.8	192.168.2.6
May 13, 2021 06:52:50.043855906 CEST	56023	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:50.095726013 CEST	53	56023	8.8.8.8	192.168.2.6
May 13, 2021 06:52:51.260823965 CEST	58384	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:51.309694052 CEST	53	58384	8.8.8.8	192.168.2.6
May 13, 2021 06:52:52.307389021 CEST	60261	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:52.356153011 CEST	53	60261	8.8.8.8	192.168.2.6
May 13, 2021 06:52:53.287791967 CEST	56061	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:53.336656094 CEST	53	56061	8.8.8.8	192.168.2.6
May 13, 2021 06:52:54.436913013 CEST	58336	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:54.485773087 CEST	53	58336	8.8.8.8	192.168.2.6
May 13, 2021 06:52:56.280595064 CEST	53781	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:56.329334974 CEST	53	53781	8.8.8.8	192.168.2.6
May 13, 2021 06:52:57.384898901 CEST	54064	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:57.436517954 CEST	53	54064	8.8.8.8	192.168.2.6
May 13, 2021 06:52:58.382720947 CEST	52811	53	192.168.2.6	8.8.8.8
May 13, 2021 06:52:58.431531906 CEST	53	52811	8.8.8.8	192.168.2.6
May 13, 2021 06:53:05.328180075 CEST	55299	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:05.382451057 CEST	53	55299	8.8.8.8	192.168.2.6
May 13, 2021 06:53:10.005081892 CEST	63745	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:10.062433958 CEST	53	63745	8.8.8.8	192.168.2.6
May 13, 2021 06:53:23.768367052 CEST	50055	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:23.819917917 CEST	53	50055	8.8.8.8	192.168.2.6
May 13, 2021 06:53:32.538383007 CEST	61374	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:32.597445965 CEST	53	61374	8.8.8.8	192.168.2.6
May 13, 2021 06:53:34.344424963 CEST	50339	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:34.454890013 CEST	53	50339	8.8.8.8	192.168.2.6
May 13, 2021 06:53:35.110593081 CEST	63307	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:35.210896969 CEST	53	63307	8.8.8.8	192.168.2.6
May 13, 2021 06:53:35.861603022 CEST	49694	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:35.921525002 CEST	53	49694	8.8.8.8	192.168.2.6
May 13, 2021 06:53:35.971358061 CEST	54982	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:36.028095007 CEST	53	54982	8.8.8.8	192.168.2.6
May 13, 2021 06:53:36.350294113 CEST	50010	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:36.412396908 CEST	53	50010	8.8.8.8	192.168.2.6
May 13, 2021 06:53:37.044521093 CEST	63718	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:37.106242895 CEST	53	63718	8.8.8.8	192.168.2.6
May 13, 2021 06:53:37.662574053 CEST	62116	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:37.722450018 CEST	53	62116	8.8.8.8	192.168.2.6
May 13, 2021 06:53:38.497231960 CEST	63816	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:38.554431915 CEST	53	63816	8.8.8.8	192.168.2.6
May 13, 2021 06:53:39.298732042 CEST	55014	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:39.351965904 CEST	53	55014	8.8.8.8	192.168.2.6
May 13, 2021 06:53:40.335757971 CEST	62208	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:40.392875910 CEST	53	62208	8.8.8.8	192.168.2.6
May 13, 2021 06:53:40.950741053 CEST	57574	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:41.001692057 CEST	53	57574	8.8.8.8	192.168.2.6
May 13, 2021 06:53:46.875204086 CEST	51818	53	192.168.2.6	8.8.8.8
May 13, 2021 06:53:46.932452917 CEST	53	51818	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:54:09.397334099 CEST	56628	53	192.168.2.6	8.8.8.8
May 13, 2021 06:54:09.455780029 CEST	53	56628	8.8.8.8	192.168.2.6
May 13, 2021 06:54:17.573807001 CEST	60778	53	192.168.2.6	8.8.8.8
May 13, 2021 06:54:17.633224964 CEST	53	60778	8.8.8.8	192.168.2.6
May 13, 2021 06:54:20.831334114 CEST	53799	53	192.168.2.6	8.8.8.8
May 13, 2021 06:54:20.907432079 CEST	53	53799	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5500 Parent PID: 5940

General

Start time:	06:52:44
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\6333f266_by_Libranalysis.dll'
Imagebase:	0x1070000
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: 6036 Parent PID: 5500

General

Start time:	06:52:44
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\6333f266_by_Libranalysis.dll',#1
Imagebase:	0x2a0000
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: 5796 Parent PID: 6036

General

Start time:	06:52:45
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\6333f266_by_Libranalysis.dll',#1
Imagebase:	0xd60000
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: 00000002.00000002.432220422.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6608 Parent PID: 5796

General

Start time:	06:53:13
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5796 -s 764
Imagebase:	0xcc0000
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	70851717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.tmp.xml	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90DB.tmp.csv	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BD9.tmp.txt	success or wait	1	70844BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 4d 2f 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....M/.`.....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 d8 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 a4 16 00 00 2d 2f 9d 60 07 00 00 00 10 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....-/.`.................. ....0..=.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.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 cf ee 00 10 0e 37 08 03 00 00 00 00 00 00 00 00 cf ee 00 10 04 8b 0c b2 44 f9 d3 00 9b ea 00 10 23 00 00 00 82 02 01 00 94 f8 d3 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........7................. D.......#...........+.........	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	168	bc 03 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 9b ea 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 8b 0c b2 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	....%..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	20	11 00 00 00 70 c9 07 03 00 00 00 00 04 00 00 00 bc 34 00 00	....p............4..	success or wait	17	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	4	7c fa 1a 03	|...	success or wait	16	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	976	bc b1 e5 77 d6 c9 e3 77 64 02 00 00 aa aa aa aa 10 00 00 00 c4 fc b2 04 90 fd b2 04 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 c0 fa 02 00 c0 fa 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 c0 fa 02 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 09 09 03 00 00 00 00 00 00 00 00 20 09 08 03 00 00 fa 02 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 02 fa 02 6c fa aa 04 b8 07 08 03 74 fa aa 04 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..................... ..@..w@..w................d... ....d......................... ....T...l. ......t......................	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.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 00 00 00 00 cf ee 00 10 00 00 00 00 28 ea d3 00 bc 9a e5 77 23 00 00 00 02 02 00 00 98 e8 d3 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...+. ..+.......................... (......w#...........+.........	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	48	e4 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 c0 fa 02 00 00 00 00 30 fc b2 04 00 00 00 00 d0 03 00 00 84 a0 00 00 cc 02 00 00 dc 30 00 00	....0..... ....0..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 92 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 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 60 75 02 00 00 00 00 00 60 cc 02 00 00 00 00 4b 4d 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 28 71 03 00 00 00 00 00 3b 71 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 43 1b 00 00 00 00 00 6d bb 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00	..Ht.....0...U..s@...%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....`u.....`..... KM.....(q.....;q .....C.....m..... @.....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER85CF.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 a8 33 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 56 b0 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.....`...V..... ..T.....@...	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.7.9.6.<./.P.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 31 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.2.1.0.5.<./.U.p.t.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 36 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.>.2.7.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 34 00 34 00 36 00 37 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.>.9.2.4.4.6.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 34 00 34 00 36 00 37 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.>.9.2.4.4.6.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.1.8.4.6.4.0.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 34 00 34 00 30 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.>.1.8.4.4.4.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.6.4.8.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.3.7.6.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 37 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.7.3.6.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 38 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.8.1.8.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 37 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.7.3.6.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.0.3.6.<./.P.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 35 00 32 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.>.3.2.5.2.2.<./.U.p.t.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 36 00 32 00 37 00 38 00 34 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.>.5.7.4.6.2.7.8.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 38 00 37 00 31 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.8.7.1.3.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 38 00 37 00 30 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.7.0.7.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 38 00 33 00 33 00 38 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.3.3.8.5.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.5.7.6.8.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 35 00 30 00 38 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.>.5.0.8.8.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 34 00 38 00 32 00 31 00 37 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.>.2.4.8.2.1.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 39 00 32 00 31 00 39 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.>.3.5.9.2.1.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 34 00 38 00 32 00 31 00 37 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.>.2.4.8.2.1.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 65 00 71 00 79 00 75 00 75 00 78 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.>.e.q.y.u.u.x.,. .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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 65 00 71 00 79 00 75 00 75 00 78 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.>.e.q.y.u.u.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 39 00 37 00 31 00 35 00 37 00 35 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.>.1.5.6.9.7.1.5.7.5.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 33 00 3a 00 31 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.3.:.5.3.:.1.7.Z.".>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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 35 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 39 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 37 00 32 00 31 00 38 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 37 00 32 00 31 00 38 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.=.".3.5.4.". .P.I.D.=.".5.7.9.6.". .U.p.t.i.m.e.M.S.=.".2.7.2.1.8.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.7.2.1.8.". .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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 30 00 32 00 63 00 32 00 35 00 63 00 31 00 2d 00 36 00 31 00 62 00 35 00 2d 00 34 00 65 00 33 00 32 00 2d 00 39 00 63 00 34 00 36 00 2d 00 38 00 66 00 37 00 31 00 65 00 61 00 66 00 38 00 33 00 34 00 62 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.0.2.c.2.5.c.1.-.6.1.b.5.-.4.e.3.2.-.9.c.4.6.-.8.f.7.1.e.a.f.8.3.4.b.e.<./.G.u.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 33 00 3a 00 31 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:.5.3.:.1.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D71.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER90ED.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\Report.wer	unknown	2	ff fe	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f22de7ba5f00b6c5d192ecc210ad9988f6_82810a17_19eaab78\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 32 00 36 00 35 00 32 00 37 00 31 00 30 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.3.2.6.5.2.7.1.0.4.	success or wait	1	7084497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	708636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70861FB2	RegCreateKeyExW
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	708636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	708636BF	unknown
\REGISTRY\A\{3811809b-ad91-649c-ce0b-45e2a7c2562a}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	708636BF	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 9B EA 00 10 02 00 00 00 01 00 00 00 04 8B 0C B2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	70861FE8	RegSetValueExW

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

Disassembly

Code Analysis