ID: 413031
Sample Name: 931f389a_by_Libranalysis.dll
Cookbook: default.jbs
Time: 06:41:17
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

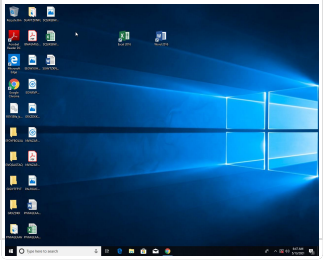
Analysis Report 931f389a_by_Libranalysis.dll

Overview

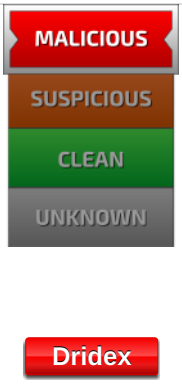
General Information

Sample Name:	931f389a_by_Libranalysis.dll
Analysis ID:	413031
MD5:	931f389af3eac90..
SHA1:	f0444b6d18303e4.
SHA256:	a98b3bccd362cfb..
Infos:	

Most interesting Screenshot:



Detection



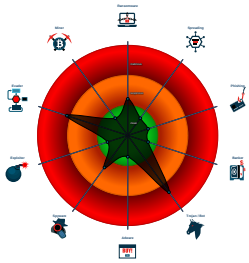
Dridex

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

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6300 cmdline: loaddll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6312 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6332 cmdline: rundll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 7164 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6332 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "203.114.109.124:443",
    "82.165.145.100:6601",
    "94.177.255.18:8172"
  ],
  "RC4 keys": [
    "BwjTiXD0nMT8wuL0lzuDMT1lwajgYLnSPMpMch1H2fk8H",
    "Zn2kewZlGvQs4cF0q7SiWd3gnwzXSWs561WqoqBWjN3RtNQTcvkRtcHJba3Ed"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.278464354.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

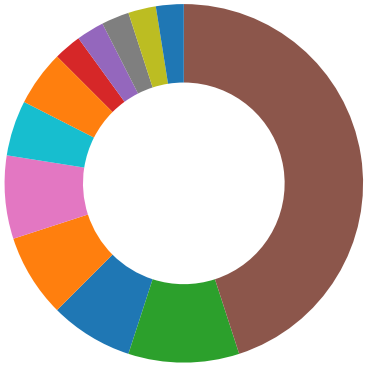
Unpacked PEs

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

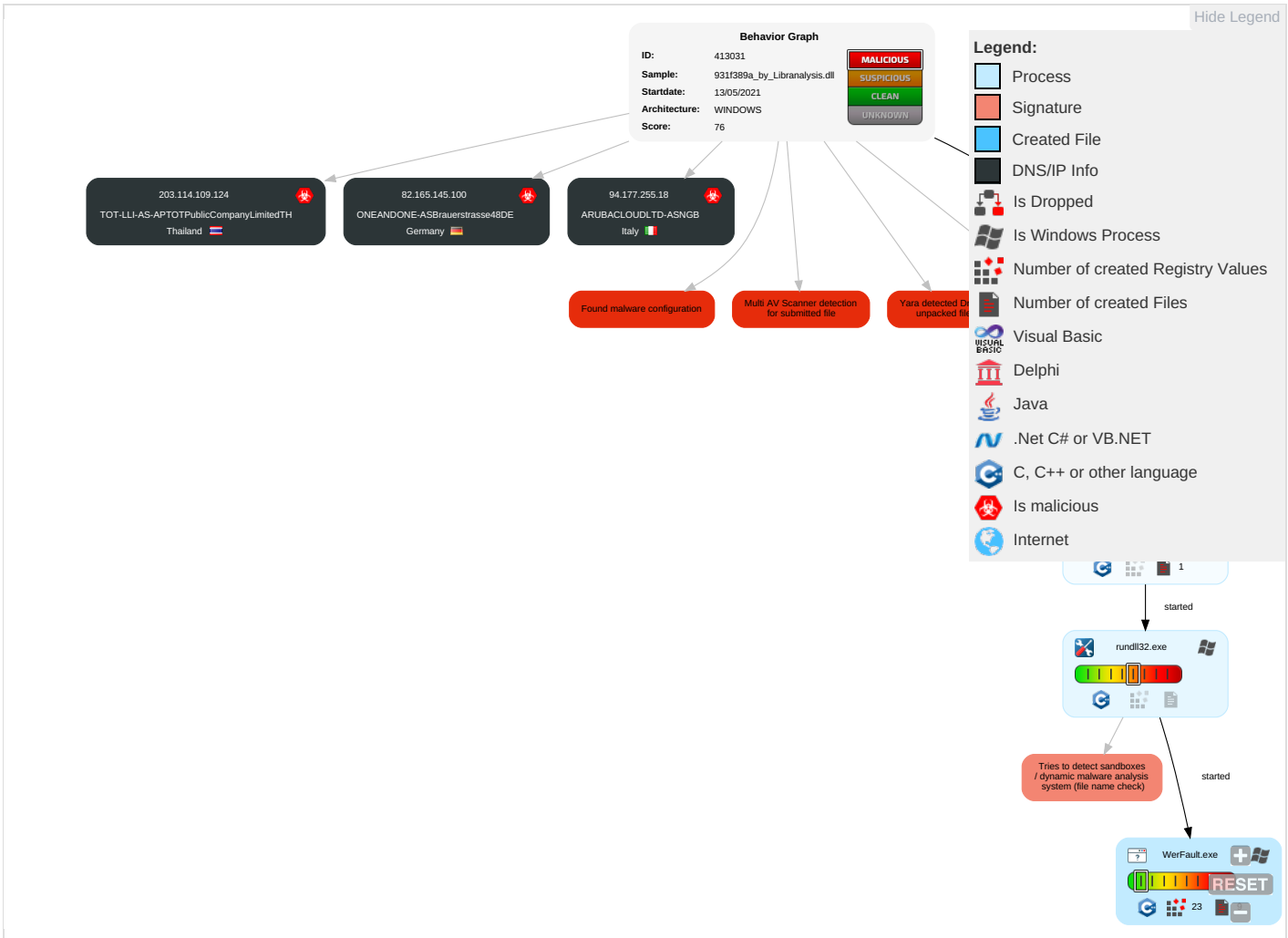
Malware Analysis System Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 1 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Phor 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
931f389a_by_Libranalysis.dll	62%	ReversingLabs	Win32.Infostealer.Dridex	
931f389a_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.d70000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	931f389a_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	931f389a_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	931f389a_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	931f389a_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.177.255.18	unknown	Italy		199883	ARUBACLOUDLTD-ASNGB	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
82.165.145.100	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413031
Start date:	13.05.2021
Start time:	06:41:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	931f389a_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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.5% (good quality ratio 49%) • Quality average: 66.1% • Quality standard deviation: 36.8%
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
94.177.255.18	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	
203.114.109.124	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	
82.165.145.100	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
TOT-LLI-AS-APTOTPublicCompanyLimitedTH	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.109.124
ARUBACLOUDLTD-ASNGB	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	7807c65b_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\Report.wer

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

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12678
Entropy (8bit):	3.767917651489283
Encrypted:	false
SSDEEP:	192:80in0oXdPYHBUZMX4jed+p4R/u7soS274ItWc/:niZXaBUZMX4je//u7soX4ItWc/
MD5:	0F833384788FBF02239D5BF900377952
SHA1:	08D4D45067C5FA95D01996E3D520792D3DF40CE2
SHA-256:	1D0B86DCC498F45DA27951A057D0ED3C6E98FEFCA079FC02471E75D1338C4FCE
SHA-512:	F2116801295CAD347F86257EFC4049816863C56EFAF8FC60115662B051EF0545882DC5C7C993063EC1BDE0197400F9CB51DD0027B4805F79F75ECE824D341EF3
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.7.0.8.9.6.9.5.5.5.3.6.....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.=.1.3.2.6.5.3.8.7.0.9.0.7.4.2.4.2.9.1.....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.=.9.9.6.7.3.a.8.6.-.c.7.4.d.-.4.d.4.0.-.a.a.5.9.-.7.8.c.b.0.2.c.2.8.c.d.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.3.6.2.7.3.8.9.-.9.d.0.a.-.4.6.e.8.-.8.b.c.4.-.2.3.e.5.e.6.6.d.e.b.f.5.....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.=.0.0.0.0.1.8.b.c.-.0.0.0.1.-.0.0.1.7.-.d.2.9.2.-.8.2.1.3.f.e.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\WER3D67.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:44:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	54316
Entropy (8bit):	2.1957690037770448
Encrypted:	false
SSDEEP:	192:iIfNik/opRJmgKCQ922mb0jq6GVLtlT5r80vxqnVVd7Wk:LloJmgZQ9VBmfLt7r80voVVdSk
MD5:	81BD7E584F32823B79B9135439A96529
SHA1:	71FE751C3DAC67BCDBE8EC7F4F2336A1004C045B
SHA-256:	07D4D2AA2116C5CF62768B2472F2FC77F9B82E96CD365C6491E4CC0794A29D26
SHA-512:	642CD4A35A43A819E882A3F2A3FEF423F0B11DE07E36789B2F488E87336D23D95FBC062762D475C5CEEC9179E093DAA067B44AEC855C843B58B000215A34DAB
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....R-.`.....U.....B..... .....GenuineIntelW.....T.....4-.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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):	3.695988416727486
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihz6pp6YVZ6JgmfTMZSOCprR889brOsfUZm:RrlsNiF6n6Yb6JgmfToSHprNfH
MD5:	72D490349328C423AA949A3DCFD73A54
SHA1:	36FE351BF9E7CD1B7240C2571052E3BAFE84356E
SHA-256:	8BDE1E898084F39729CCEC4919F24C423A073E3EDC7ABCD35B4B5B92ABA6DDEB
SHA-512:	1E5EEBCD7C0215AB03C94C4F415DE408CE17806A0F590A36E020C127310C17C5EE7934E8B81EEC0E80B74E5414409674FCFCB94241A2FBB67EDDF08C01F470I7
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4663

C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp.xml	
Entropy (8bit):	4.478506650961813
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9C7+vWSC8BR8fm8M4JCdsqNntFB+q8/vNFnRN4SrSLd:uITfTtRSNcJAN5wNhDWLd
MD5:	5AA4B262F08C0A74BE26BC9C755A3531
SHA1:	FD0126AED35E68085F8469BC6FEFBE8DECFC6CF7
SHA-256:	01E2D19FAC9A66E26F553E26C16B3E438911EEBBAB0DB4058E84BB46A5B35467
SHA-512:	56CE8DD0BF9E00614450EAA1B290B9C2FFB4F273973360682BEA52324C08086B4FCCF1031A562ECB8568706970A30203FA4C673AEB1BED341D6A5108ADBD44C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987775" />.. <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):	7.583609842944269
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:	931f389a_by_Libranalysis.dll
File size:	166856
MD5:	931f389af3eac907ce78eb6219e28f47
SHA1:	f0444b6d18303e468f993f5fad350f585e811650
SHA256:	a98b3bccd362cfbac2de3f8dfc80e041ce2aa327fcd07480ac60db93cdb980cd
SHA512:	2cb3f259b94d78a4c6e9a4b6259aff7beee2c223e89324fd824a416eb146ce59bbc0eae6e054d6e8cc7ea5d82bd59d40ee1fb7941aaced3ebe22e292a4938b78
SSDEEP:	3072:w/FbrEzD9N+RiMB00c9/74DXE+JgaV7IPx+e6O/pPtaLOi:CbrE1kvcB74DXZ2Mel3i
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.%.0zK.0zK.0zK.0zJ.}{K...3..{K.....P{K...3..zK.V....zK...1..{K.....zK.Rich0zK.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10023130
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F80 [Thu May 13 01:23:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0

General

File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	35893a758d71a4b313745582f88cfeb6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 12/6/2020 4:00:00 PM 12/7/2021 3:59:59 PM
Subject Chain	• CN=STAND ALONE MUSIC LTD, O=STAND ALONE MUSIC LTD, STREET="23 Cameo House, 11 Bear Street", L=LONDON, PostalCode=WC2H 7AS, C=GB
Version:	3
Thumbprint MD5:	BE49CFBB4B6B5F4638C9EC0872B04B7C
Thumbprint SHA-1:	A5887C72B22F81884E714EDEC711E52FDC60EA37
Thumbprint SHA-256:	F680FAB6A9D21E8E76003C5C28B3C5084866D7AC85CF0CFB5AAA02F69EE99F1E
Serial:	3B777165B125BCCC181D0BAC3F5B55B3

Entrypoint Preview

Instruction
xor eax, eax
add eax, 00002234h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
jne 00007F9B9CC6DD49h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Instruction
mov eax, 00000000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2672a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x267f8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2b000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x27400	0x17c8	.pdata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2c000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x222ac	0x22400	False	0.761077212591	data	7.58875564719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x2a76	0x2c00	False	0.793323863636	data	7.44946265271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x27000	0x3390	0x1800	False	0.722330729167	MMDF mailbox	7.18721728982	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x3a0	0x400	False	0.423828125	data	3.05991849143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x250	0x400	False	0.517578125	data	4.09990016339	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

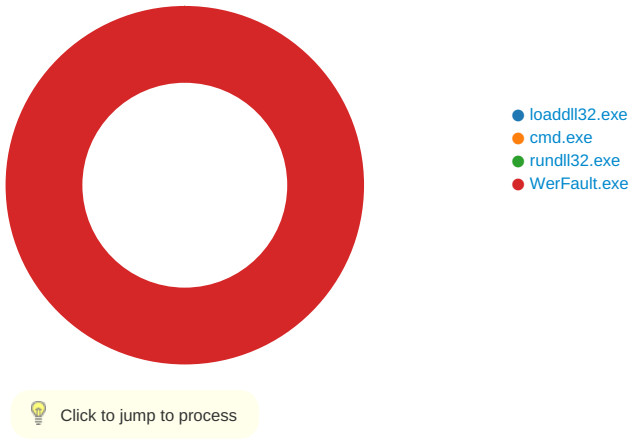
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:44:12.577707052 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:12.626393080 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 06:44:14.327168941 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:14.386575937 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:44:15.289531946 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:15.338237047 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:44:17.123238087 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:17.172045946 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 06:44:18.400201082 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:18.452877998 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 06:44:19.595256090 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:19.643973112 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 06:44:20.765018940 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:20.813649893 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 06:44:21.896961927 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:21.945755959 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 06:44:22.958178997 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:23.007927895 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 06:44:24.505443096 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:24.554088116 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 06:44:25.642714977 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:25.691549063 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 06:44:27.310323954 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:27.359205961 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 06:44:28.658951044 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:28.707739115 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 06:44:30.190633059 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:30.239568949 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 06:44:31.495590925 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:31.544250965 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 06:44:32.822066069 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:32.870812893 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 06:44:34.110713005 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:34.160830021 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 06:44:39.323682070 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:39.381303072 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 06:44:46.624577045 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:46.683784008 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 06:44:51.381170034 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:51.429817915 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 06:44:57.037770987 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 06:44:57.112030983 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 06:45:05.177565098 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 06:45:05.237354994 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 06:45:08.076153040 CEST	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:45:08.126866102 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 06:45:36.440610886 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 06:45:36.498054981 CEST	53	61292	8.8.8.8	192.168.2.3
May 13, 2021 06:45:42.144957066 CEST	63619	53	192.168.2.3	8.8.8.8
May 13, 2021 06:45:42.203439951 CEST	53	63619	8.8.8.8	192.168.2.3
May 13, 2021 06:45:58.731776953 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 06:45:58.807385921 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 06:46:13.545567989 CEST	61946	53	192.168.2.3	8.8.8.8
May 13, 2021 06:46:13.611226082 CEST	53	61946	8.8.8.8	192.168.2.3
May 13, 2021 06:46:15.472661018 CEST	64910	53	192.168.2.3	8.8.8.8
May 13, 2021 06:46:15.546410084 CEST	53	64910	8.8.8.8	192.168.2.3
May 13, 2021 06:47:04.606384039 CEST	52123	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:04.718715906 CEST	53	52123	8.8.8.8	192.168.2.3
May 13, 2021 06:47:05.308516026 CEST	56130	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:05.406044006 CEST	53	56130	8.8.8.8	192.168.2.3
May 13, 2021 06:47:05.990883112 CEST	56338	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:06.040884972 CEST	53	56338	8.8.8.8	192.168.2.3
May 13, 2021 06:47:06.578264952 CEST	59420	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:06.639640093 CEST	53	59420	8.8.8.8	192.168.2.3
May 13, 2021 06:47:07.421514988 CEST	58784	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:07.480796099 CEST	53	58784	8.8.8.8	192.168.2.3
May 13, 2021 06:47:08.255023956 CEST	63978	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:08.315576077 CEST	53	63978	8.8.8.8	192.168.2.3
May 13, 2021 06:47:09.325052023 CEST	62938	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:09.384069920 CEST	53	62938	8.8.8.8	192.168.2.3
May 13, 2021 06:47:10.477483034 CEST	55708	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:10.534603119 CEST	53	55708	8.8.8.8	192.168.2.3
May 13, 2021 06:47:11.575618982 CEST	56803	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:11.635651112 CEST	53	56803	8.8.8.8	192.168.2.3
May 13, 2021 06:47:12.122282028 CEST	57145	53	192.168.2.3	8.8.8.8
May 13, 2021 06:47:12.179724932 CEST	53	57145	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6300 Parent PID: 5704

General

Start time:	06:44:19
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll'
Imagebase:	0x830000
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: 6312 Parent PID: 6300

General

Start time:	06:44:20
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
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: 6332 Parent PID: 6312

General

Start time:	06:44:20
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\931f389a_by_Libranalysis.dll',#1
Imagebase:	0xda0000
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: 00000002.00000002.278464354.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 7164 Parent PID: 6332

General

Start time:	06:44:48
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6332 -s 764
Imagebase:	0xf70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70111717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7010497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp	success or wait	1	7010497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	success or wait	1	70104BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	success or wait	1	70104BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.tmp.xml	success or wait	1	70104BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1DF.tmp.csv	success or wait	1	70104BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1EF.tmp.txt	success or wait	1	70104BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 52 2d 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....R-.`.....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.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 b0 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 bc 18 00 00 34 2d 9d 60 07 00 00 00 11 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B..... .... ..GenuineIntelW.....T... ....4-.`..... .....0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 d0 91 01 10 20 35 0c 03 ff ff ff ff d0 91 01 10 3a 32 00 02 cc f8 af 00 d0 91 01 10 23 00 00 00 47 02 01 00 48 f8 af 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 aa aa aa aa	....+...S...+. ..+........... 5..........:2.. ....#...G...H...+.........	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	168	c0 18 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 d0 91 01 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3b 32 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 ba 26 00 00	....;2.......... ....&..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	20	13 00 00 00 00 c0 ea 02 00 00 00 00 00 10 00 00 ea 35 00 00	................5..	success or wait	19	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	4096	d0 e9 af 00 00 00 b0 00 00 40 af 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 c0 ea 02 00 00 00 00 bc 18 00 00 c0 18 00 00 00 00 00 00 b0 09 0d 03 00 90 ea 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 d6 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.........@.................... ....p.w..............	success or wait	18	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 da 00 a0 7b f0 77 88 17 0b 03 00 00 00 00 00 00 0b 03 a0 79 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 40 77 00 00 00 00 00 00 00 00 00 00 a6 00 00 00 00 00 f8 7b f0 77 ff ff ff ff 0f 00 00 00 00 00 87 7f 00 00 00 00 30 07 87 7f 00 00 97 7f 28 02 98 7f 50 06 99 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 60 66 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 f0 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.............{.w.............y .w..............@w................. {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa d0 91 01 10 00 00 00 00 e0 e9 af 00 bc 9a e5 77 23 00 00 00 16 02 00 00 50 e8 af 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#.......P...+.........	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	48	a4 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 eb 02 00 00 00 00 cc f8 07 03 00 00 00 00 34 07 00 00 ea 65 00 00 cc 02 00 00 ea 31 00 00	....P............ ..4....e.......1..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	53	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 a0 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 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 80 30 02 00 00 00 00 00 a0 9a 02 00 00 00 00 f0 55 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 18 eb 00 00 00 00 00 00 9d 63 03 00 00 00 00 00 cb 77 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 8a dc 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 94 eb 21 00 00 00 00	..Ht.....0...U..s@...&..... .....B.....B?..... .....#..... ..@A.....Zb..... ....0..... .U.....c .....w.....!..... @.....!....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D67.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 cc 07 00 00 05 00 00 00 34 01 00 00 b6 34 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 14 b6 00 00 15 00 00 00 ec 01 00 00 2c 1e 00 00 16 00 00 00 98 00 00 00 18 20 00 00	..............`..........4. ...4.........T.......8..... ....T..........`..... ..,..... ..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.3.3.2.<./.P.i.d.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 39 00 31 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.9.9.1.4.<./.U.p.t.i.m.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 39 00 33 00 35 00 39 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.>.1.2.9.3.5.9.8.7.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 39 00 33 00 35 00 31 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.>.1.2.9.3.5.1.6.8.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 35 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.5.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 34 00 36 00 31 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.6.1.7.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 34 00 36 00 31 00 37 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.6.1.7.6.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.4.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.4.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 32 00 32 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.2.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 32 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.0.0.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 36 00 31 00 33 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.3.1.7.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 36 00 31 00 33 00 39 00 39 00 30 00 34 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.>.6.1.3.9.9.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 36 00 31 00 33 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.1.3.1.7.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.3.1.2.<./.P.i.d.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 32 00 39 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.>.3.0.2.9.5.<./.U.p.t.i.m.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.3.4.4.0.5.1.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.1.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 35 00 30 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.>.3.7.1.5.0.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 37 00 30 00 32 00 37 00 38 00 34 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.>.3.7.0.2.7.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 32 00 32 00 34 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.>.5.2.2.4.<./.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 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.>.3.4.1.6.0.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 36 00 37 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.7.6.1.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 33 00 34 00 31 00 36 00 30 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.>.3.4.1.6.0.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 70 00 6a 00 63 00 74 00 67 00 6b 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.>.p.j.c.t.g.k.,. .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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 70 00 6a 00 63 00 74 00 67 00 6b 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.>.p.j.c.t.g.k.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 33 00 35 00 37 00 37 00 32 00 37 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.8.3.5.7.7.2.7.8.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 34 00 34 00 3a 00 35 00 30 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.:.4.4.:.5.0.Z.".>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 34 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 33 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 37 00 33 00 37 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 37 00 33 00 37 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.5.". .P.I.D.=.".6.3.3.2.". .U.p.t.i.m.e.M.S.=.".2.7.3.7.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.7.3.7.4.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 39 00 36 00 37 00 33 00 61 00 38 00 36 00 2d 00 63 00 37 00 34 00 64 00 2d 00 34 00 64 00 34 00 30 00 2d 00 61 00 61 00 35 00 39 00 2d 00 37 00 38 00 63 00 62 00 30 00 32 00 63 00 32 00 38 00 63 00 64 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.9.6.7.3.a.8.6.-.c.7.4.d.-.4.d.4.0.-.a.a.5.9.-.7.8.c.b.0.2.c.2.8.c.d.f.<./.G.u.i.d.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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 34 00 34 00 3a 00 35 00 30 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.:.4.4.:.5.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4056.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	7010497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER40E3.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	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\Report.wer	unknown	2	ff fe	..	success or wait	1	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	184	7010497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79dc4f33d2677f24610e49eb7f526d71a7c260_82810a17_1bb947b7\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 32 00 36 00 30 00 30 00 36 00 34 00 35 00 36 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.6.0.0.6.4.5.6.0.	success or wait	1	7010497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	701236BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70121FB2	RegCreateKeyExW
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701043D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	701236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	701236BF	unknown
\REGISTRY\A\{feebef6b-f11f-6bb0-53a8-0afe7483a0b1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	701236BF	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 D0 91 01 10 02 00 00 00 00 00 00 00 3B 32 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	70121FE8	RegSetValueExW

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

Disassembly

Code Analysis