

JoeSandbox Cloud BASIC



ID: 392885

Sample Name: IHUVPJ4hXu.dll

Cookbook: default.jbs

Time: 23:47:38

Date: 19/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report IHUVPJ4hXu.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Malware Analysis System Evasion:	5
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	11
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	14
General	14
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	15
Data Directories	15
Sections	16
Resources	16
Imports	16
Version Infos	16
Possible Origin	16

Network Behavior	16
Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loaddll32.exe PID: 6908 Parent PID: 5872	17
General	17
File Activities	17
Analysis Process: cmd.exe PID: 6916 Parent PID: 6908	17
General	17
File Activities	18
Analysis Process: rundll32.exe PID: 6948 Parent PID: 6916	18
General	18
File Activities	18
File Read	18
Analysis Process: rundll32.exe PID: 7032 Parent PID: 6908	18
General	18
File Activities	19
File Read	19
Analysis Process: WerFault.exe PID: 1424 Parent PID: 6908	19
General	19
File Activities	19
File Created	19
File Deleted	20
File Written	20
Registry Activities	42
Key Created	42
Key Value Created	42
Disassembly	42
Code Analysis	43

Analysis Report IHUVPJ4hXu.dll

Overview

General Information

Sample Name:

IHUVJPJ4hXu.dll

Analysis ID:

392885

MD5:

5b10d906d4ad48..

SHA1:

9995dad015c20..

SHA256:

61f03287190b9ce.

Tags:

40111 Dridex

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

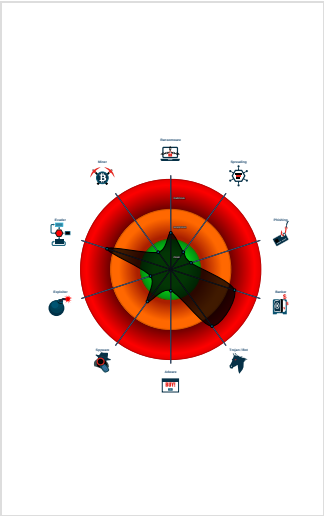
Dridex Dropper

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Dridex dropper found
- Found malware configuration
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con...
- Machine Learning detection for samp...
- Tries to delay execution (extensive O...
- Tries to detect sandboxes / dynamic...
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec...
- Contains functionality to call native f...
- Contains functionality to check if a d...
- Contains functionality to query locale...

Classification



Startup

System is w10x64

- loadll32.exe (PID: 6908 cmdline: loadll32.exe 'C:\Users\user\Desktop\IHUVJPJ4hXu.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
 - cmd.exe (PID: 6916 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\IHUVJPJ4hXu.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 6948 cmdline: rundll32.exe 'C:\Users\user\Desktop\IHUVJPJ4hXu.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - rundll32.exe (PID: 7032 cmdline: rundll32.exe 'C:\Users\user\Desktop\IHUVJPJ4hXu.dll',ReadLogRecord MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - WerFault.exe (PID: 1424 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6908 -s 416 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 40111,
  "C2 list": [
    "94.247.168.64:443",
    "159.203.93.122:8172",
    "50.116.27.97:2303"
  ],
  "RC4 keys": [
    "V0w9c7u110XYjoFF2SzRWnchNob7Sec1HxEVgBrFF",
    "5gZeCc8o5cQELWnF44Ik184W6MoZ25098Ro7kPT2itFhVdxWiT70K4o4YnFUN4mL"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1042008848.000000006EE B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.1041480154.000000006EE B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

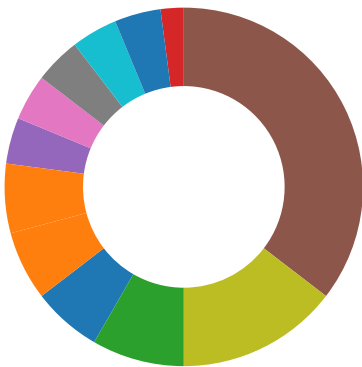
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.6eeb0000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.6eeb0000.3.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

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Dridex dropper found

Yara detected Dridex unpacked file

Malware Analysis System Evasion:



Tries to delay execution (extensive OutputDebugStringW loop)

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 2	Virtualization/Sandbox Evasion 2 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop (Insecure Network Communication)
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Virtualization/Sandbox Evasion 2 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 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IHUVPJ4hXu.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loadDll32.exe.2ce0000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
4.2.rundll32.exe.4a00000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
2.2.rundll32.exe.27f0000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ansicon.adoxavze.com/6	IHUVJPJ4hXu.dll	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.203.93.122	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
50.116.27.97	unknown	United States		63949	LINODE-APLinodeLLCUS	true
94.247.168.64	unknown	Sweden		43948	GLESYS-ASSE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392885
Start date:	19.04.2021
Start time:	23:47:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IHUVJPJ4hXu.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:	12
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:	mal80.bank.troj.evad.winDLL@8/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.1% (good quality ratio 92.2%) • Quality average: 80.3% • Quality standard deviation: 26.2%
HCA Information:	• Successful, ratio: 82% • 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
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, wermgr.exe, backgroundTaskHost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
159.203.93.122	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	u3A1eWFqLE.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	IHUVJPJ4hXu.dll	Get hash	malicious	Browse	
	CTkT1fRtQv.dll	Get hash	malicious	Browse	
	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	qMus8K6kXx.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1UmI5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1Uml5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	
50.116.27.97	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	u3A1eWFqLE.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	IHUVJPJ4hXu.dll	Get hash	malicious	Browse	
	CTkT1fRtQv.dll	Get hash	malicious	Browse	
	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	qMus8K6kXx.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1Uml5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1Uml5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	
94.247.168.64	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	u3A1eWFqLE.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	IHUVJPJ4hXu.dll	Get hash	malicious	Browse	
	CTkT1fRtQv.dll	Get hash	malicious	Browse	
	BJKPKLUPiD.dll	Get hash	malicious	Browse	
	RuRxpMUPN7.dll	Get hash	malicious	Browse	
	qMus8K6kXx.dll	Get hash	malicious	Browse	
	gsG7jGFk3l.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1Uml5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	
	Ce28zthEz1.dll	Get hash	malicious	Browse	
	15sV4KdrCN.dll	Get hash	malicious	Browse	
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	
	1Uml5PSg3K.dll	Get hash	malicious	Browse	
	9eYYTTIVYi.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 159.203.93.122
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 159.203.93.122
	u3A1eWFqLE.dll	Get hash	malicious	Browse	• 159.203.93.122
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 159.203.93.122
	IHUVJPJ4hXu.dll	Get hash	malicious	Browse	• 159.203.93.122
	CTkT1fRtQv.dll	Get hash	malicious	Browse	• 159.203.93.122
	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 159.203.93.122
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 159.203.93.122
	qMus8K6kXx.dll	Get hash	malicious	Browse	• 159.203.93.122
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 159.203.93.122
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 159.203.93.122
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 159.203.93.122

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 159.203.93.122
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 159.203.93.122
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 159.203.93.122
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 159.203.93.122
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 159.203.93.122
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 159.203.93.122
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 159.203.93.122
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 159.203.93.122
LINODE-APLinodeLLCUS	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 50.116.27.97
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 50.116.27.97
	u3A1eWFqLE.dll	Get hash	malicious	Browse	• 50.116.27.97
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 50.116.27.97
	IHUVpJ4hXu.dll	Get hash	malicious	Browse	• 50.116.27.97
	CTkT1fRtQv.dll	Get hash	malicious	Browse	• 50.116.27.97
	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 50.116.27.97
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 50.116.27.97
	qMus8K6kXx.dll	Get hash	malicious	Browse	• 50.116.27.97
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 50.116.27.97
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 50.116.27.97
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 50.116.27.97
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 50.116.27.97
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 50.116.27.97
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 50.116.27.97
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 50.116.27.97
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 50.116.27.97
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 50.116.27.97
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 50.116.27.97
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 50.116.27.97
GLESYS-ASSE	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 94.247.168.64
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 94.247.168.64
	u3A1eWFqLE.dll	Get hash	malicious	Browse	• 94.247.168.64
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 94.247.168.64
	IHUVpJ4hXu.dll	Get hash	malicious	Browse	• 94.247.168.64
	CTkT1fRtQv.dll	Get hash	malicious	Browse	• 94.247.168.64
	BJKPKLUPiD.dll	Get hash	malicious	Browse	• 94.247.168.64
	RuRxpMUPN7.dll	Get hash	malicious	Browse	• 94.247.168.64
	qMus8K6kXx.dll	Get hash	malicious	Browse	• 94.247.168.64
	gsG7jGFk3l.dll	Get hash	malicious	Browse	• 94.247.168.64
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 94.247.168.64
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 94.247.168.64
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 94.247.168.64
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 94.247.168.64
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 94.247.168.64
	Ce28zthEz1.dll	Get hash	malicious	Browse	• 94.247.168.64
	15sV4KdrCN.dll	Get hash	malicious	Browse	• 94.247.168.64
	Yvl2Gke3pv.dll	Get hash	malicious	Browse	• 94.247.168.64
	1Uml5PSg3K.dll	Get hash	malicious	Browse	• 94.247.168.64
	9eYTTIVYi.dll	Get hash	malicious	Browse	• 94.247.168.64

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	9236
Entropy (8bit):	3.76307669365411
Encrypted:	false
SSDEEP:	96:uvFFzagV9XyAy9hAIQC5Q56tpXIQcQ6c6n+hcEZcw3P+a+z+HbHgX6eugtYsaV9S:PgagLHUb+hbjbUq/u7seS274ltb2w
MD5:	8EA89827A7C91C74F16454CD1583B219
SHA1:	F646BAA6237FC936E695E804CD7DB2EE058F19F6
SHA-256:	FF71BBF2019EF2FE118A8C5AD9CF28B87B065D09435CA41628AF7CB9276B3184
SHA-512:	B9C224211B8365DB877B0D4788945A0D44D21A0752EB1BFB78E78BAAF219C99E0E070FFF20EE77D703941A9650306A23A33B92B755B5523F576B71FE15D4944C
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=B.E.X.....E.v.e.n.t.T.i.m.e.=1.3.2.6.3.3.4.2.6.6.0.1.3.1.8.2.4.3.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=0.f.4.9.4.6.e.b.-d.6.5.b.-4.b.b.c.-b.e.5.2-.0.9.3.8.9.e.2.4.8.e.e.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=3.b.9.5.d.f.7.5.-c.2.d.0.-4.f.3.f.-8.e.9.0.-f.b.e.1.6.2.7.d.8.5.9.1.....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.=l.o.a.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.a.f.c.-0.0.0.1-.0.0.1.b.-0.a.8.c.-6.a.b.8.6.5.3.5.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=2.0.2.1!/0.4!/0.4.:1.0.:5.0.:5.4.!0.!l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.l.d.=4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Apr 19 21:51:01 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	24442
Entropy (8bit):	2.705625380028496
Encrypted:	false
SSDEEP:	96:5kJ8NGYCMz4l7RgAaqztiti+WDckhFrZOiHBof83ln4WinWidoZwl4irlBDqFMp:/Jz77R1Naq3mP4uBofg9AnicBDEMHWWx
MD5:	0E56582E070BE327B983F5576BF5EEFC
SHA1:	C37F2FBE91352D492E1414F14B79BC432C6781E4
SHA-256:	11D6155EE7A0B35D150E8F05C8C4C66BF83F641A14A719B20D8141421EB33B05
SHA-512:	E43E15BAF83C2290BE60A49F265375F92DE76AF2653F4D3F1699E67C09DF7827CDEC2E2F2D49C813D5B8CBEF73EAAFC97C61F968A19CE8672BE4EE055B427A8
Malicious:	false
Reputation:	low
Preview:	MDMP.....E.)`.....U.....B.....GenuineIntelW.....T.....}`.....0.....W...E.u.r.o.p.e..S.t.a.n.d.a.r.d..T.i.m.e.....W...E.u.r.o.p.e..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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):	8362
Entropy (8bit):	3.6936080688136395
Encrypted:	false
SSDEEP:	192:RrI7r3GLNiNi6MAc6YrySUJEW1gmfnS1D+pBe89bJksfsjm:RrlsNi/6MAc6YeSUJESgmfnS1SJXf1
MD5:	0F9E519BF14EC034CF30C553938D3E40
SHA1:	35B9E0526F5F462BC45E6929BA83493A7BC5205D
SHA-256:	9258F8E44E279FF557C93F7BA164E1462356F4F55C1C32303F3EACF192B9FC72
SHA-512:	33F530ECFEDBB1D8821FB8CAE2CE8E6C7149A4D2DD60C49414491BBD1D7CA1B496D1DAB2703AAF938F545E9BA9FF8BD2723266DC71ABFF53754D61E4FB0E466F
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>.6.9.0.8.</P.i.d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp.xml	
Size (bytes):	4658
Entropy (8bit):	4.434914226771162
Encrypted:	false
SSDEEP:	48:cvlwSD8zsVJgtWI96MrWSC8Bb8fm8M4JVMFO+q8v7bKcQlcQw6Urid:uITfvlNSNKJJKHKkw68ld
MD5:	491BBC2C92D5BFBBDFED7C5585353D01
SHA1:	87771873E6088D218D864C6758B52A34D8CC6D79
SHA-256:	3B0FF6C244C9A89701A9EE4E7A4ABE6CFC6A8AEE1F423BC68EDDAC890A80F9EB
SHA-512:	32700A5A3526A9E603363D5AC93DE106A38242891528EA36FDECEE91F8A4BAD26BCE47EC4911191A085E3E1F74FDA3F1AC86E61DA1401559466798D1FF4DF9B
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="verblid" 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="953701" />.. <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):	7.5485592804649535
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:	IHUVJPJ4hXu.dll
File size:	163840
MD5:	5b10d906d4ad48a9910a8cc551b2e697
SHA1:	9995dadcd015c2003cdfc34c081a5f185aad6263
SHA256:	61f03287190b9ce1e91fab24eddc302f411813ac49230d2e99335952eb3addc0
SHA512:	a31772c3ecbb7289e6fc43e81314c426dcc7671e1b9ee664ff31dbca2d921e9cab1f09d744661d11a70952e4278642769a98a9804314159c47cfa709f5197d20
SSDEEP:	3072:xWX2ljzpm+PncPeY8+O3AU3HRIHPh3UGfXy0BHNklvScbQQ2y0iNM0+y+N0tc:x42IfzNPnoeY8j3AsHGPXpHNj6rByM3
File Content Preview:	MZ.....@.....[.]...[.]...[.]...@2...[.]...T...S.z[.]...@...[.]...T...V/C...V/E...Rich[}.....PE..L...}'.....!.....f.....D.....P....@.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x424410
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x607DE4E1 [Mon Apr 19 20:15:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b84fd50f2389cfd5bd83e2cf062986d1

Entrypoint Preview

Instruction

[illegible]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1001	0x0	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2768c	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x340	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x14c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x25040	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x3c	.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	0x2356e	0x23600	False	0.761560015459	data	7.55877156847	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2842	0x2a00	False	0.791573660714	data	7.53164670284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x28000	0x3588	0x1600	False	0.783380681818	MMDF mailbox	7.34765964879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x340	0x400	False	0.390625	data	2.73456990044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x14c	0x200	False	0.62890625	data	4.21021599876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x2e0	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, OpenSemaphoreW, LoadLibraryExA, GetModuleHandleW, OutputDebugStringA, GetProfileSectionW
OPENG32.dll	glTexSubImage1D
ole32.dll	CreateStreamOnHGlobal
USER32.dll	TranslateMessage
ADVAPI32.dll	RegLoadAppKeyW

Version Infos

Description	Data
LegalCopyright	Freeware
InternalName	ANSI32
FileVersion	1.66
CompanyName	Jason Hood
Comments	http://ansicon.adoxa.vze.com/
ProductName	ANSICON
ProductVersion	1.66
FileDescription	ANSI Console
OriginalFilename	ANSI32.dll
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

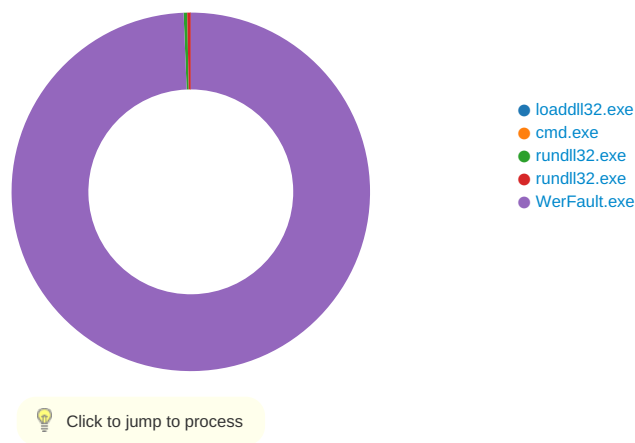
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loadDll32.exe PID: 6908 Parent PID: 5872

General

Start time:	23:48:23
Start date:	19/04/2021
Path:	C:\Windows\System32\loadDll32.exe
Wow64 process (32bit):	true
Commandline:	loadDll32.exe 'C:\Users\user\Desktop\IHUVPJ4hXu.dll'
Imagebase:	0x1150000
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: 6916 Parent PID: 6908

General

Start time:	23:48:23
-------------	----------

Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\IHUVPJ4hXu.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 6948 Parent PID: 6916

General

Start time:	23:48:24
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\IHUVPJ4hXu.dll',#1
Imagebase:	0x280000
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: 00000002.00000002.1041480154.000000006EEB1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEC5E36	ReadFile

Analysis Process: rundll32.exe PID: 7032 Parent PID: 6908

General

Start time:	23:48:55
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\IHUVPJ4hXu.dll',ReadLogRecord
Imagebase:	0x280000
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: 00000004.00000002.1042008848.000000006EEB1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEC5E36	ReadFile

Analysis Process: WerFault.exe PID: 1424 Parent PID: 6908

General	
Start time:	23:50:56
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6908 -s 416
Imagebase:	0x850000
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	6F581717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_!oaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6F57497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6F57497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp.xml	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1A8.tmp.csv	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB62D.tmp.txt	success or wait	1	6F57497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 45 fb 7d 60 a4 05 12 00 00 00 00 00	MDMP.....E.}.....	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.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 2c 14 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 fc 1a 00 00 a7 fa 7d 60 09 00 00 00 15 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 0d 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	U.....B..... ..GenuineIntelW.....T...}0.....W... ..E.u.r.o.p.e. .S.t.a.n.d.a.r.d.. ..T.i.m.e.....W... E.u.r.o.p.e. .D.a.y.l.i.g.h.t.. ..T.i.m.e.....	success or wait	1	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D8.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 24 0a 00 00 48 07 00 00 0e 00 00 00 3c 00 00 00 6c 11 00 00 05 00 00 00 64 00 00 00 c8 1c 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 c8 10 00 00 fa 4e 00 00 15 00 00 00 ec 01 00 00 a8 11 00 00 16 00 00 00 98 00 00 00 94 13 00 00	...4.....\$.H.....<. ..l.....d.....`.. ...8.....T..... ..N.....	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.0.8.</.P.i.d.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 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.>.I.o.a.d.d.I.I.3.2...e.x.e.</.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 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	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 38 00 32 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.5.8.2.0.7.<./U.p.t.i.m.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	<.l.p.t.E.n.a.b.l.e.d.>.0.<./l.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 39 00 33 00 34 00 32 00 38 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.9.3.4.2.8.4.8.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 33 00 38 00 34 00 33 00 32 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.>.5.1.3.8.4.3.2.0.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 36 00 36 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.>.1.6.6.9.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 36 00 32 00 35 00 34 00 35 00 39 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.>.6.2.5.4.5.9.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 35 00 38 00 32 00 34 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.8.2.4.5.1.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 30 00 38 00 39 00 39 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 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.>.1.0.8.9.9.2.<./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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 30 00 31 00 31 00 32 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>.1.0.1.1.2.8.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 37 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>.1.7.6.3.2.<./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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 37 00 33 00 36 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>.1.7.3.6.0.<./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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 36 00 37 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.1.6.7.9.3.6.0.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 32 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.9.1.2.8.3.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 31 00 36 00 37 00 39 00 33 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.6.7.9.3.6.0.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./P.i.d.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 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.>.e.x.p.l.o.r.e.r...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 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>.8.0.0.0.4.0.0.5.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 36 00 34 00 36 00 30 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e>.7.6.4.6.0.0.2.<./U.p.t.i.m.e>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	78	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 30 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 30 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.="0".h.o.s.t.="3.4.4.0.4.">.0.<./W.o.w.6.4.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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.>.4.2.9.4.9.6.7.2.9.5.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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.>.4.2.9.4.9.6.7.2.9.5.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	76	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 36 00 30 00 36 00 35 00 31 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.>.6.0.6.5.1.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	100	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 31 00 30 00 36 00 35 00 32 00 34 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.5.2.4.6.7.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	84	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 31 00 30 00 34 00 30 00 36 00 37 00 30 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.0.6.7.0.7.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 39 00 38 00 30 00 37 00 35 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 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.>.9.8.0.7.5.2.<./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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 38 00 37 00 32 00 30 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.>.8.8.7.2.0.8.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 37 00 35 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.7.5.8.9.6.<./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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 36 00 39 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.9.1.9.2.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	78	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 33 00 34 00 38 00 37 00 33 00 33 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.8.7.3.3.4.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	94	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 38 00 34 00 35 00 37 00 33 00 34 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.>.3.8.4.5.7.3.4.4.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	74	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 38 00 37 00 33 00 33 00 34 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.>.3.4.8.7.3.3.4.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./E.v.e.n.t.T.y.p.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	9	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 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.>.l.o.a.d.d.l.l.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 71 00 79 00 71 00 6b 00 6f 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.p.q.y.q.k.o.,.I.n.c...<./S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 71 00 79 00 71 00 6b 00 6f 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.p.q.y.q.k.o.7.,.1.<./S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 33 00 37 00 38 00 33 00 31 00 39 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.3.7.8.3.1.9.6. <./O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>-.0.1...0.0. <./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 42 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.B.<./F.l.a.g.s.>.	success or wait	3	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 34 00 2d 00 31 00 39 00 54 00 32 00 31 00 3a 00 35 00 31 00 3a 00 30 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.B.a.s.e.T.i.m.e.="2.0.2.1.-0.4.-1.9.T.2.1.:5.1.:0.1.Z.">.	success or wait	1	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	270	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 39 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 32 00 30 00 33 00 30 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 31 00 35 00 32 00 30 00 33 00 30 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 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68	<.P.r.o.c.e.s.s. .A.s.I.d.= ". 3.5.5.". .P.I.D.= ".6.9.0.8.". .U.p.t.i.m.e.M.S.= ".1.5.2.0.3.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".1.5.2.0.3.0.". .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	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 66 00 34 00 39 00 34 00 36 00 65 00 62 00 2d 00 64 00 36 00 35 00 62 00 2d 00 34 00 62 00 62 00 63 00 2d 00 62 00 65 00 35 00 32 00 2d 00 30 00 39 00 33 00 38 00 39 00 65 00 32 00 34 00 38 00 65 00 65 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.f.4.9.4.6.e.b.-. d.6.5.b.-.4.b.b.c.-.b.e.5.2.-. 0.9.3.8.9.e.2.4.8.e.e.9. <./G.u.i.d.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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 34 00 2d 00 31 00 39 00 54 00 32 00 31 00 3a 00 35 00 31 00 3a 00 30 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2. 0.2.1.-.0.4.-.1.9.T.2.1.:5.1. :0.1.Z.<./C.r.e.a.t.i.o.n.T. i.m.e.>.	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEBB.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	6F57497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1AA.tmp.xml	unknown	4658	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"?>.. 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	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\Report.wer	unknown	2	ff fe	..	success or wait	1	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\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	149	6F57497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_259aeac81dd625d6a234674e48313673fc16336_160cf2be_05e4b6b9\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 30 00 33 00 39 00 32 00 36 00 35 00 39 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1. 6.0.3.9.2.6.5.9.7.	success or wait	1	6F57497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5091a42b-71a5-36b4-4e10-f677790e7e7d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F591FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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 00 EB 6E 02 00 00 00 08 00 00 00 00 00 EB 6E 00	success or wait	1	6F591FE8	RegSetValueExW

Disassembly
