ID: 413035
Sample Name:
c2b6efb1_by_Libranalysis
Cookbook: default.jbs
Time: 06:40:30
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

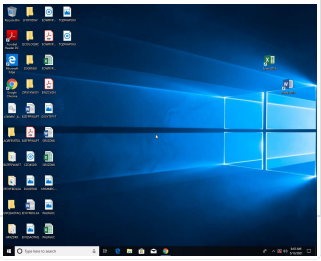
Analysis Report c2b6efb1_by_Libranalysis

Overview

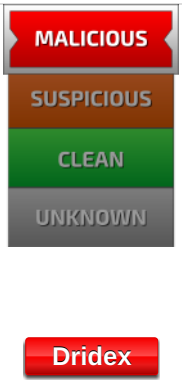
General Information

Sample Name:	c2b6efb1_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413035
MD5:	c2b6efb1b15eab8.
SHA1:	fab251bf2316a77..
SHA256:	2626744dae6404..
Infos:	

Most interesting Screenshot:



Detection



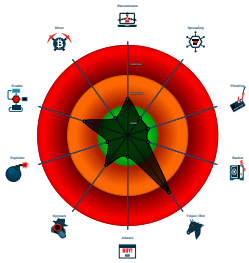
Dridex

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

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6352 cmdline: loaddll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6360 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6372 cmdline: rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5472 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.328088849.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

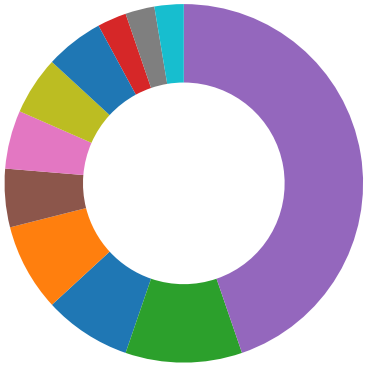
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

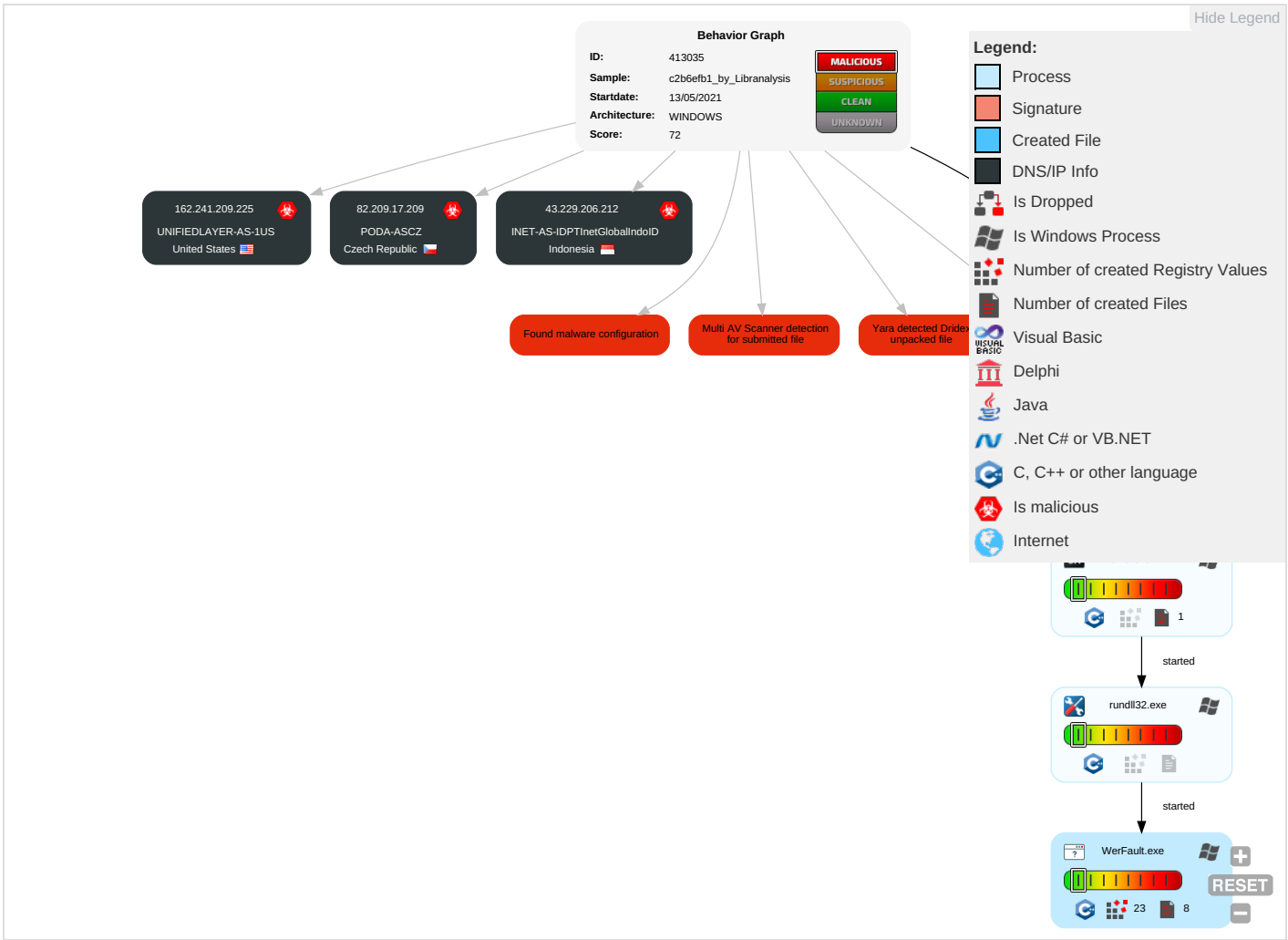
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

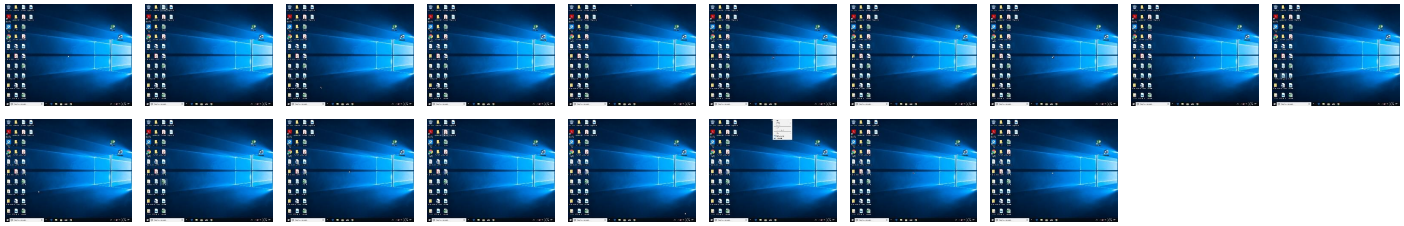
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
c2b6efb1_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
c2b6efb1_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.3240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	

Domains and IPs

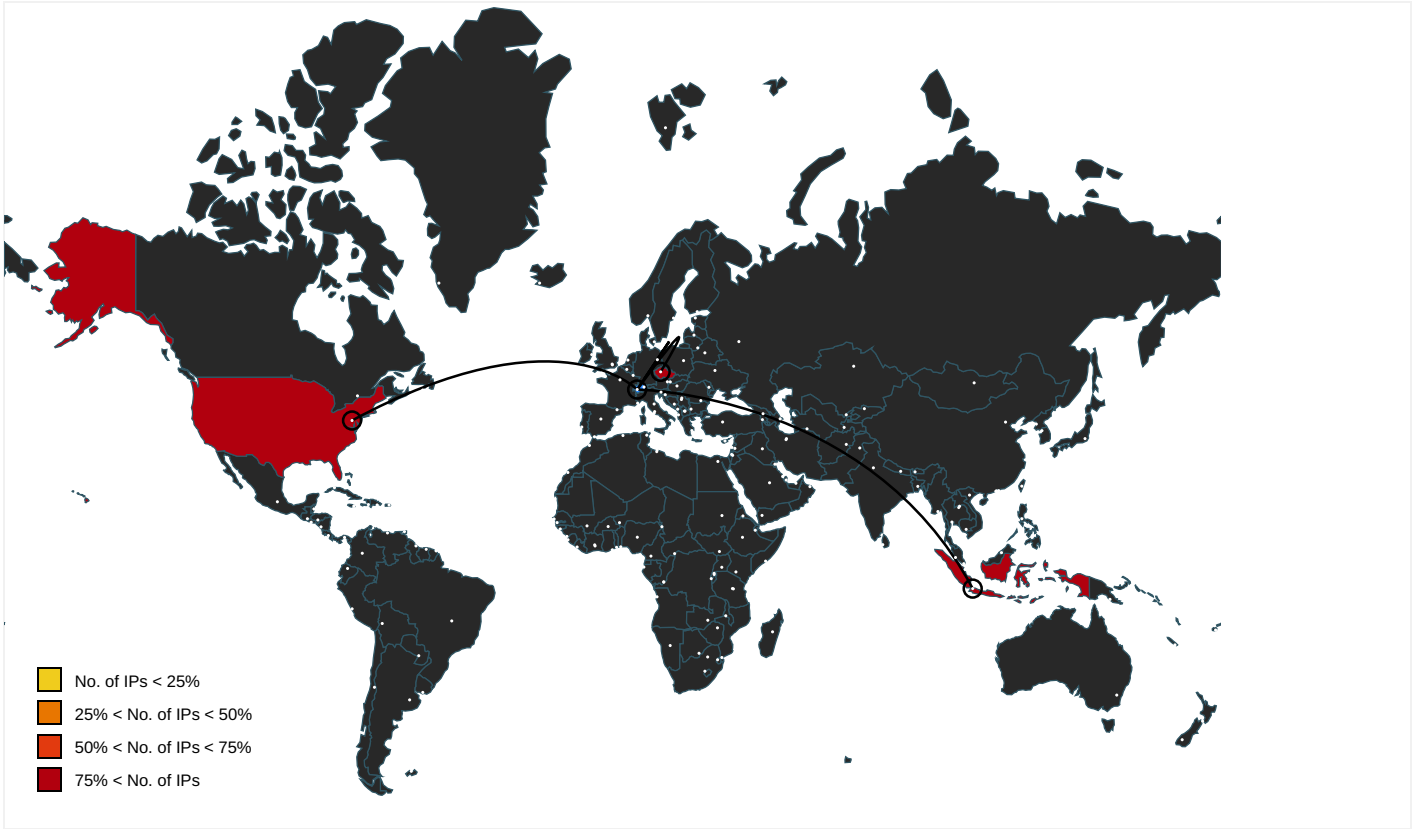
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.microsoft	WerFault.exe, 0000000E.0000000 3.321854224.0000000004B7C000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.209.17.209	unknown	Czech Republic		30764	PODA-ASCZ	true
162.241.209.225	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
43.229.206.212	unknown	Indonesia		24532	INET-AS-IDPTInetGlobalIndoID	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413035
Start date:	13.05.2021
Start time:	06:40:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c2b6efb1_by_Libranalysis (renamed file extension from none to 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
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.7% (good quality ratio 85.2%) • Quality average: 67.2% • Quality standard deviation: 35%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
06:42:05	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	• 82.209.17.209
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	• 43.229.206.212
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	SecuriteInfo.com.Trojan.Win32.Save.a.22467.dll	Get hash	malicious	Browse	• 162.241.209.225
	94fca788_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e97b5e6f_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	modified
Size (bytes):	12486
Entropy (8bit):	3.7668343270882034
Encrypted:	false
SSDEEP:	192:pmi10oXLcHBUZMX4jed+Oe/u7sFS274ItWck:0ibXoBUZMX4jeC/u7sFX4ItWck
MD5:	6DFFBF5C6C00C1F5231B95602FFFB08F
SHA1:	8352661017ED09F6E0B75035563905C11E0B8BC4
SHA-256:	E6E783C8275327F0708FCAFFE43A449098821A3869ACF60845A5FF0FEAE6AF99
SHA-512:	DE09700139F04851C83958DE016D83537FBAB341ABABBEDA7C5A08A99164C35EA640FD1EE12DDED66A0E7B23A21BCB0ACA5D88B26529671D3C995987E83D7208
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.6.9.1.5.4.0.2.4.9.8.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.6.9.2.3.1.5.2.4.8.8.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.8.6.4.c.7.c.d.-.e.3.4.b.-.4.9.3.3.-.a.f.a.a.-.6.6.e.8.e.1.6.c.7.f.e.4.....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.=.e.9.1.9.0.4.a.1.-.d.a.c.8.-.4.b.8.e.-.9.7.d.6.-.a.3.9.1.d.6.f.6.b.d.1.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.e.4.-.0.0.0.1.-.0.0.1.6.-.2.4.c.b.-.2.b.a.9.f.d.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:41:58 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40226
Entropy (8bit):	2.3001854423819768
Encrypted:	false
SSDEEP:	192:PyAjYVeFBzx+jO1UCTsBQ3Qorx7JASZmSMUnaWP:2VeXzx+K2VBCQANASNX
MD5:	9A5337C702117F71954CB8A514E1B797
SHA1:	8F5A30385EF6E1E77EE649E0C1EC64E4B4169787
SHA-256:	B1C93FE264AED4B7C4220357616E1CD6F3C1B173E34F3AB22CB5967FACDCAC57
SHA-512:	2BEC9F9C7C11C44E44F2C83DE37126A29F78A681FA707D6C84503ECD71C756808B9C29E8FA4E7745CC03591E898007D4EEA3B8371BDD01516450618883D45BC
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....,.`.....U.....B.....x.....GenuineIntelW.....T.....,.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8292
Entropy (8bit):	3.6961104874289186
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilh6Y16Y4r6ZfEgmfTnVS4CprI89bPnIsfdlm:RrlsNiz666Yc6ZsgmfTVS1Pn7fe
MD5:	D43EB03CA72FCC164D25CEFAF3F922E9
SHA1:	5355AB889FD72B8FB7BAE68A844C9B3AB9555A11
SHA-256:	3E5F75CCB67ED05ACBF75DB5A4DC121B52991F37958F0193EEAB4DC4465EAC17
SHA-512:	E80517A8FD403835B70D3E6299665FE0825E74ABD2C4FD7AF945D57085FD49A9F31E970FE3B3AB8A896C6FA866E21A45FB356BD646DD610E78DF400EEC94AED
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4663
Entropy (8bit):	4.475667455882159
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUNJgtWI9bzWSC8BT8fm8M4JCdsLNrFPS+q8/uNFqMF4SrSjd:uITfSECSN+J9NENN0MFDWjd
MD5:	824510D40FAC56FC1FA50C58D1BDA86D
SHA1:	370A3E2ED67C97AC20F14AF08F2A8AC392292B53
SHA-256:	36704DCDC342D43018950348A683F1097ED865B685535E98FDF19892F0D5ED6C
SHA-512:	6791EBCEB3BC58014638AA78BA2CA046818D64190C2DAD261F595DD6015454FBC5FF114F5C29DFE7661DD9F65155B4D11FBECD755C900435D50035256C66F62
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987772" />.. <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):	7.513878784862757
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:	c2b6efb1_by_Libranalysis.dll
File size:	167424
MD5:	c2b6efb1b15eab83bcec9afd875fbb34
SHA1:	fab251bf2316a77c53f3b92ad016ed9697f4f14a
SHA256:	2626744dae64045e445cbab9a2a225827d362ef6a0c20ea56b67dcec779857e
SHA512:	632e3cb1ff7220b5ecc5800ecef4d6ebd69ff7a21d040e76a0a5dce9f06103b98bc3e60b05a34bf2e240ec91b89f028a0436f7b3760e3cb291327d123c5dfb66
SSDEEP:	3072:89F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:89F6rQXvFczvYpQP

General

File Content Preview:	MZ.....@.....\.....!..L.!This program cannot be run in DOS mode....$.....Xm.o...<...<...<.U!<...<..B<r..<...<...<rQ!<...<;..<...<;..<3..<au.<...<szt<"..<Rich...<.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10024cc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F8B [Thu May 13 01:23:23 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx
mov dword ptr [10029730h], eax
mov eax, esi
mov dword ptr [10029728h], eax
jne 00007FD29CB7D4A6h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Instruction
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x389c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x33c	data		

Imports

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

Version Infos

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

Network Behavior

UDP Packets

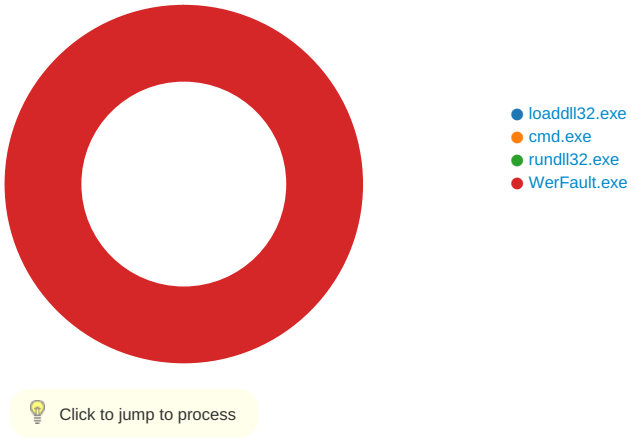
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:41:14.247447014 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:14.266599894 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:14.320542097 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 06:41:14.324110985 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 06:41:14.426280022 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:14.467561007 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:14.477844000 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 06:41:14.524830103 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 06:41:14.971554041 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:15.020358086 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 06:41:16.134031057 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:16.187882900 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 06:41:17.301340103 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:17.350217104 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 06:41:18.610131025 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:18.667332888 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 06:41:18.702156067 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:18.753598928 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 06:41:20.453843117 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:20.505477905 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 06:41:21.570756912 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:21.619580984 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 06:41:22.765757084 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:22.814429045 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 06:41:25.972207069 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:26.024183989 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 06:41:27.144186974 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:27.205585957 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 06:41:28.657772064 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:28.709431887 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 06:41:30.613554001 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 06:41:30.662189960 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 06:41:40.946412086 CEST	55161	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:41:41.006402016 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 06:42:04.115586042 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 06:42:04.164387941 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 06:42:04.823456049 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 06:42:04.900413990 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 06:42:20.571624994 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:42:20.632805109 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:42:47.428766966 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:42:47.501671076 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:42:50.097834110 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 06:42:50.156563044 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 06:43:05.950217962 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 06:43:06.015170097 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 06:43:26.050312996 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 06:43:26.122706890 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 06:43:27.071993113 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 06:43:27.140410900 CEST	53	50463	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6352 Parent PID: 5680

General

Start time:	06:41:21
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll'
Imagebase:	0xb50000
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: 6360 Parent PID: 6352

General

Start time:	06:41:21
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6372 Parent PID: 6360

General

Start time:	06:41:22
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1
Imagebase:	0xa40000
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: 00000002.00000002.328088849.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5472 Parent PID: 6372

General

Start time:	06:41:53
Start date:	13/05/2021

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 764
Imagebase:	0x380000
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	6D961717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	success or wait	1	6D954BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	success or wait	1	6D954BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.xml	success or wait	1	6D954BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABA2.tmp.csv	success or wait	1	6D954BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF1E.tmp.txt	success or wait	1	6D954BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 a6 2c 9d 60 a4 05 12 00 00 00 00 00	MDMP..... ..... ,.`.....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.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 78 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 18 00 00 82 2c 9d 60 07 00 00 00 12 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......x..... ..GenuineIntelW...........T... ....,.`.................. ....0..=.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 ca 30 00 10 40 35 26 03 ff ff ff ff ca 30 00 10 19 06 00 02 0c f7 f8 02 ca 30 00 10 23 00 00 00 03 02 01 00 88 f6 f8 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........0..@5&......0...... .....0..#...........+.........	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	168	e8 18 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 4c 25 00 00	.........................0.... ....L%..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	20	0b 00 00 00 00 80 07 03 00 00 00 00 00 10 00 00 64 2e 00 00	................d...	success or wait	11	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	4096	10 e8 f8 02 00 00 f9 02 00 40 f8 02 00 00 00 00 00 1e 00 00 00 00 00 00 00 80 07 03 00 00 00 00 e4 18 00 00 e8 18 00 00 00 00 00 00 c8 e5 25 03 00 50 07 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 9b 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.........@.................... ....%..P.......... ....p.w.............	success or wait	10	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 a4 00 a0 7b ad 77 98 17 25 03 00 00 00 00 00 00 25 03 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 ef 02 00 00 00 00 f8 7b ad 77 ff ff ff ff 07 00 00 00 00 00 29 7f 00 00 00 00 30 07 29 7f 00 00 39 7f 28 02 3a 7f 50 06 3b 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	............{.w..%.......%..y .w...............t................ {.w..........).....0.)...9. (.:.P.;.................m........ ....`f.w.. ....PS.w.........B......	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa ca 30 00 10 00 00 00 00 20 e8 f8 02 bc 9a a2 77 23 00 00 00 16 02 00 00 90 e6 f8 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+....................0...... ......w#...........+.........	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	48	f4 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 e0 07 03 00 00 00 00 74 fc d1 04 00 00 00 00 8c 03 00 00 e4 6a 00 00 cc 02 00 00 e4 2a 00 00	....t..... ....j.......*..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	51	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	752	00 00 05 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 32 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 c0 12 02 00 00 00 00 00 40 ab 02 00 00 00 00 d9 46 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 a1 dd 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 0b 22 00 00 00 00	...t.....0...U..s@..2%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....@..... .F.....F .....!..... @....."....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B85.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 6c 07 00 00 05 00 00 00 b4 00 00 00 b0 2d 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 0a 7f 00 00 15 00 00 00 ec 01 00 00 f4 1c 00 00 16 00 00 00 98 00 00 00 e0 1e 00 00	....d.....l.....-.....T.....8.....T.....`.....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.3.7.2.<./.P.i.d.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 37 00 37 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.6.7.7.8.<./.U.p.t.i.m.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 39 00 37 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.1.9.7.7.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 37 00 36 00 37 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.6.7.1.0.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 37 00 39 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.7.9.1.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 37 00 39 00 31 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.7.9.1.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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 32 00 39 00 36 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.6.8.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.4.1.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 34 00 38 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.4.8.3.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 38 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.8.1.8.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 34 00 38 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.4.8.3.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.3.6.0.<./.P.i.d.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 37 00 31 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.7.1.5.7. <./.U.p.t.i.m.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 31 00 32 00 39 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.2.9.7.9.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 35 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.5.0.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.7.8.2.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.0.9.6.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.5.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 32 00 32 00 34 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.2.2.4.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 39 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.7.9.9.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 32 00 32 00 34 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.2.2.4.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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 72 00 76 00 6f 00 75 00 6a 00 74 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.>.r.v.o.u.j.t.,. .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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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 72 00 76 00 6f 00 75 00 6a 00 74 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.>.r.v.o.u.j.t.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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 37 00 31 00 38 00 38 00 38 00 39 00 36 00 34 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.>.1.5.7.1.8.8.8.9.6.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 34 00 31 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.3.:.4.1.:.5.9.Z.".>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 38 00 34 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 38 00 34 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.8.". .P.I.D.=.".6.3.7.2.". .U.p.t.i.m.e.M.S.=.".2.9.8.4.3.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.9.8.4.3.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 38 00 36 00 34 00 63 00 37 00 63 00 64 00 2d 00 65 00 33 00 34 00 62 00 2d 00 34 00 39 00 33 00 33 00 2d 00 61 00 66 00 61 00 61 00 2d 00 36 00 36 00 65 00 38 00 65 00 31 00 36 00 63 00 37 00 66 00 65 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.8.6.4.c.7.c.d.-.e.3.4.b.-.4.9.3.3.-.a.f.a.a.-.6.6.e.8.e.1.6.c.7.f.e.4.<./.G.u.i.d.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 34 00 31 00 3a 00 35 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:.4.1.:.5.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA903.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	6D95497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB95.tmp.xml	unknown	4663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b\Report.wer	unknown	2	ff fe	..	success or wait	1	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	6D95497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1509c19b\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 37 00 35 00 35 00 32 00 33 00 34 00 31 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.5.7.5.5.2.3.4.1.3.	success or wait	1	6D95497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D9736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D971FB2	RegCreateKeyExW
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D9736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D9736BF	unknown
\REGISTRY\A\{f9633673-1faf-274d-1576-99ef7d30a75b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D9736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 CA 30 00 10 02 00 00 00 01 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D971FE8	RegSetValueExW

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

Disassembly

Code Analysis