ID: 413032
Sample Name:
a13bac07_by_Libranalysis
Cookbook: default.jbs
Time: 06:34:46
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report a13bac07_by_Libranalysis 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Dridex 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
E-Banking Fraud: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 15
Resources 15
Imports 16
Version Infos 16
Network Behavior 16

UDP Packets 16
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: loaddll32.exe PID: 660 Parent PID: 5664 17
General 17
File Activities 18
Analysis Process: cmd.exe PID: 204 Parent PID: 660 18
General 18
File Activities 18
Analysis Process: rundll32.exe PID: 5464 Parent PID: 204 18
General 18
Analysis Process: WerFault.exe PID: 6328 Parent PID: 5464 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 20
Registry Activities 41
Key Created 41
Key Value Created 41
Disassembly 42
Code Analysis 42

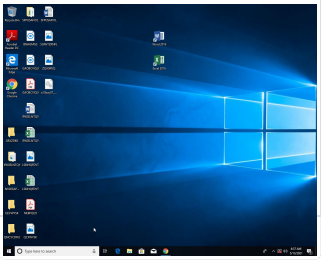
Analysis Report a13bac07_by_Libranalysis

Overview

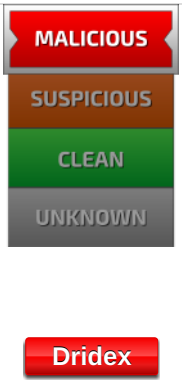
General Information

Sample Name:	a13bac07_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413032
MD5:	a13bac071a79aa..
SHA1:	307396f23bdb16e.
SHA256:	d40f0d0cbfedbf9…
Infos:	

Most interesting Screenshot:



Detection

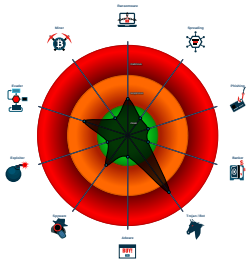


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Creates a 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: 660 cmdline: loaddll32.exe 'C:\Users\user\Desktop\a13bac07_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 204 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a13bac07_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5464 cmdline: rundll32.exe 'C:\Users\user\Desktop\a13bac07_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6328 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5464 -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
00000002.00000002.326565323.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

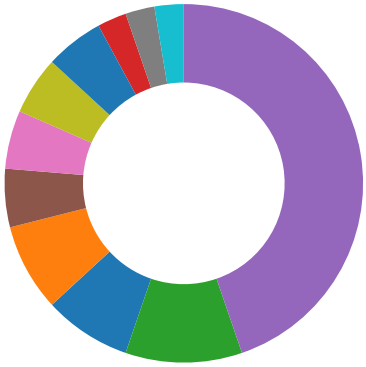
Unpacked PEs

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:

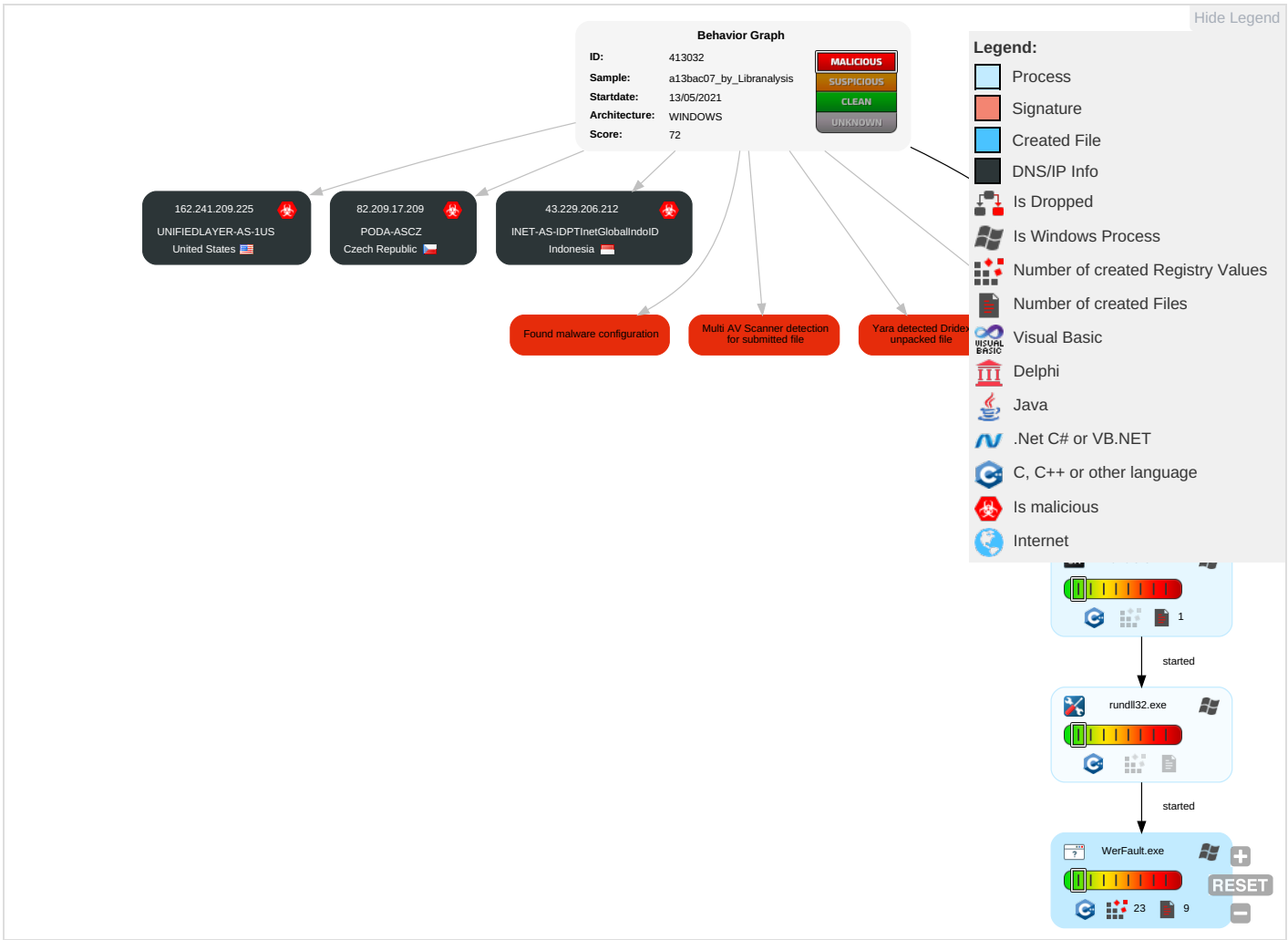
Yara detected Dridex unpacked file

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
a13bac07_by_Libranalysis.dll	32%	ReversingLabs	Win32.Trojan.Convagent	
a13bac07_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.2d20000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

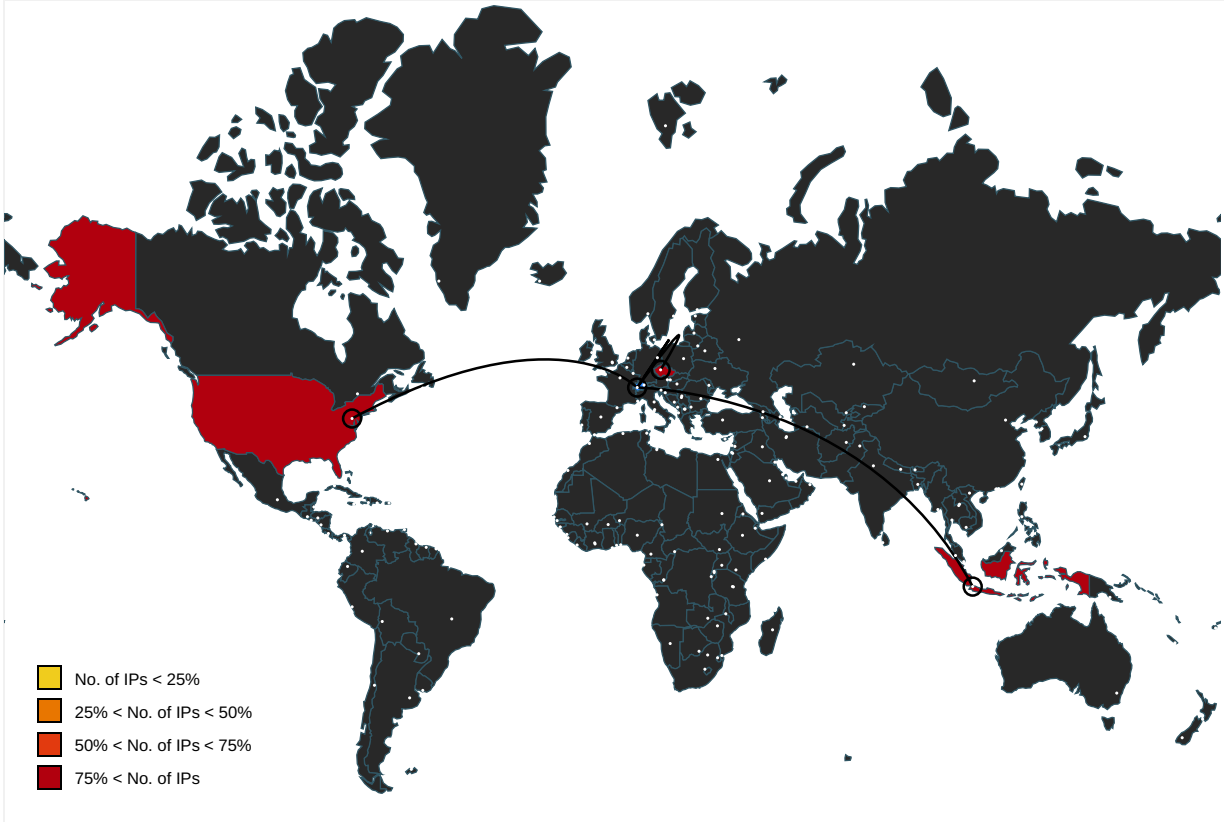
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro	WerFault.exe, 00000010.0000000 3.321687542.00000000049DE000.0 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:	413032
Start date:	13.05.2021
Start time:	06:34:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a13bac07_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:	31
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: 97.5% (good quality ratio 85.2%) • Quality average: 67.1% • 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
06:36:19	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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	
	9c168218_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	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	
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	
	9c168218_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	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	
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	
	9c168218_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	9c168218_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	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
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	9c168218_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	061020c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	f4e3325c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	09ab1bab_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	32eeda59_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	9c168218_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_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12490
Entropy (8bit):	3.766574868614943
Encrypted:	false
SSDEEP:	192:xoni20oXIcHBUZMX4jed+eG/u7sw/S274ItWc1:ciwXDBUZMX4jeS/u7sw/X4ItWc1
MD5:	83FC42943DD820C645BE619803DBAB6C
SHA1:	9B65D89EEC135C0F75CE7AC88A3641931653C54A
SHA-256:	0C6B2F932C21152549EC5BF5095E8E3680D55B3B2E404A8E8A3843F81F701BD0
SHA-512:	62FDA310FF91CB5151FCE9CFD682E45E37AE67E00B26ECA6DA9BA726D5E01BE17A30605351BF8CED53863E68A1AC28B71BB8F9268CD9B4799882D3296E27308A
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.=.1.3.2.6.5.3.8.6.5.7.1.1.6.8.2.9.7.1.....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.=.1.3.2.6.5.3.8.6.5.7.6.8.2.4.5.2.9.2.....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.=.2.1.d.3.e.6.8.4.-.e.2.6.f.-.4.e.3.a.-.8.e.4.1.-.a.3.6.f.6.3.a.9.d.4.5.d.....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.=.a.5.7.2.8.7.8.7.-.4.f.b.8.-.4.3.6.0.-.a.e.b.0.-.1.2.4.d.7.9.2.a.1.9.c.e.....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.=.0.0.0.0.1.5.5.8.-.0.0.0.1.-.0.0.1.7.-.5.6.b.6.-.0.2.d.b.f.c.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\WERB4C3.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:36:12 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40298
Entropy (8bit):	2.296614728240946
Encrypted:	false
SSDEEP:	192:4P5TjcI/JNyw3wnRUGxTq0DA4fuZokxPOa2gNrN4wYu:41Gw2qRQA4fookx72gNrau
MD5:	2BC51DB2C5FD2ADAB3D71DBC80291BE9
SHA1:	C606410B55FE91740991B275632BAB3F25A029B2
SHA-256:	F783E2E393C7E0FF4D1DE75B715F97557ADF3310BBB2782AB3B67AA4BE5EF4AC
SHA-512:	51AA9909CDD19EF568CA0695F8B96320C20D5272730DF3961FB5717C44412C3E79D5CBB0AE220398DE7605AC86D268BEEF2B2DED886E414BEA38FB309437E97A
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....L+.`.....U.....B.....x.....GenuineIntelW.....T.....X...(+.`.....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\WERBA14.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):	8290
Entropy (8bit):	3.6942631191871094
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNieXb6kX6Y4as6mlgmfT+VSfCprs89bQn4sfsJwm:RrlsNiq6k6Yu6UgmfTKS+Qnrfm
MD5:	B37DAD6F70F1242804529CF56D3DC4EA
SHA1:	21ACD14988762E68C3CBB6F8565A5124833CA35C
SHA-256:	EEEEFF07BC3AC5108868BC8DC7292CD153A79A3115E8D5E96F94B7D2488AACCA
SHA-512:	D4989EE599A507A9C61AAF89E49917154BAAE3C33A1C80196820259C48F5370FBF6BC6267A1D1FC6855E46B14238DA6DCC07C68C39ECB3F231880F0398ACF65
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.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):	4.471977093757148
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9U6WSC8BqG8fm8M4JCdsYbNrF1+q8//bNFbS4SrST6d:uITfv77SNcDJWbNzGbN9SDWT6d
MD5:	43451FDED83FDEEED82D747235502902
SHA1:	4A1DC4266E488BA57DD38546974B5CC6E3738FC9
SHA-256:	490859075DD1AAE56024CA5DFA686F7EC7ABE8C84123C6CED3454D21868373DD
SHA-512:	6B9AD30278ECCE78E9906E9C29E6B4EC6AEF422CB6B66552D95134C0B04F0B085960DAEF16AD47BF8EF801A36DFB704F611BF93721C97380D27F00EC7DFF4DB
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="987766" />.. <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):	7.5138986567652495
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:	a13bac07_by_Libranalysis.dll
File size:	167424
MD5:	a13bac071a79aa0fb0247c873294724d
SHA1:	307396f23bdb16e95559b7e3b284b3c171422424
SHA256:	d40f0d0cbfedbf90c408fce9bb4896a8dc0506c4a7a96cbef884ae3b6ba28a81
SHA512:	19bf05661295353ea95f87416617f10ff030264f59405056dd72c59b13242fff77928eea334f673938deae3722ed574f871b39dce993f8f010ddc93dc22e0624
SSDEEP:	3072:b9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:b9F6rQXvFczvYpQP

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:	0x609C7F87 [Thu May 13 01:23:19 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 00007F81B8979F16h
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	0x2cfc	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x331c	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

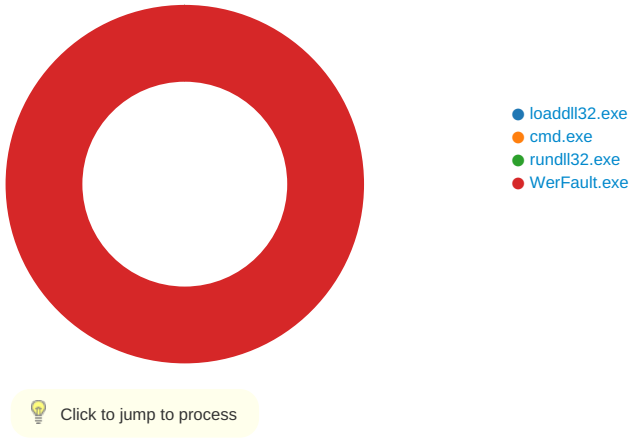
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:35:28.831042051 CEST	50848	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:28.882746935 CEST	53	50848	8.8.8.8	192.168.2.7
May 13, 2021 06:35:30.636470079 CEST	61242	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:30.696541071 CEST	53	61242	8.8.8.8	192.168.2.7
May 13, 2021 06:35:31.502312899 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:31.552221060 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 06:35:31.893702030 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:31.953366041 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 06:35:32.622545004 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:32.679706097 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 06:35:33.606673956 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:33.655508995 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 06:35:34.788621902 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:34.848835945 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 06:35:35.609113932 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:35.657855034 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 06:35:36.568620920 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:36.618711948 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 06:35:40.602864981 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:40.654355049 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 06:35:41.507028103 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:41.555802107 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 06:35:42.861546040 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:42.910366058 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 06:35:44.098795891 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:44.155852079 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 06:35:45.021817923 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:45.070501089 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 06:35:46.105458021 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:46.154844046 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 06:35:46.931651115 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:46.983153105 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 06:35:47.853450060 CEST	54008	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:35:47.910646915 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 06:35:49.268815041 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:49.317478895 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 06:35:54.289191008 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:54.304825068 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:54.350476980 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 06:35:54.356234074 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 06:35:55.308988094 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:55.359586954 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 06:35:56.259566069 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:56.311026096 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 06:35:57.240835905 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 06:35:57.289766073 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 06:36:18.286436081 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 06:36:18.337126017 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 06:36:18.567270041 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 06:36:18.626694918 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 06:36:38.104127884 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 06:36:38.162513018 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 06:37:10.642518997 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:37:10.699832916 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 06:37:22.070606947 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 06:37:22.129375935 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 06:37:40.816149950 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 06:37:40.984183073 CEST	53	59310	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 660 Parent PID: 5664

General

Start time:	06:35:35
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\a13bac07_by_Libranalysis.dll'
Imagebase:	0xd90000
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: 204 Parent PID: 660

General

Start time:	06:35:35
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\a13bac07_by_Libranalysis.dll',#1
Imagebase:	0x870000
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: 5464 Parent PID: 204

General

Start time:	06:35:36
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\a13bac07_by_Libranalysis.dll',#1
Imagebase:	0x820000
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: 00000002.00000002.326565323.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6328 Parent PID: 5464

General

Start time:	06:36:07
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5464 -s 764
Imagebase:	0x1b0000
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	6D251717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D24497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.tmp.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE58.tmp.csv	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC176.tmp.txt	success or wait	1	6D244BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 4c 2b 9d 60 a4 05 12 00 00 00 00 00	MDMP........ ....L+.`........	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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 54 05 00 00 f7 03 00 00 58 15 00 00 28 2b 9d 60 08 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 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	.....U...........B......x..... ..GenuineIntelW...........T... ....X...(+.`.................. ....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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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 c0 36 df 02 ff ff ff ff ca 30 00 10 19 06 00 02 b4 fb 8b 02 ca 30 00 10 23 00 00 00 03 02 01 00 30 fb 8b 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	....+...S...+. ..+........0...6.......0...... .....0..#.......0...+.........	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	168	80 16 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 4c 25 00 00	........................0.... ....L%..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	20	0c 00 00 00 00 50 b5 02 00 00 00 00 98 04 00 00 74 2e 00 00	.....P..........t...	success or wait	12	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 82 00 a0 7b 3b 77 d0 17 de 02 00 00 00 00 00 00 de 02 a0 79 3b 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fa 73 00 00 00 00 00 00 00 00 00 00 7f 00 00 00 00 00 f8 7b 3b 77 ff ff ff ff 07 00 00 00 00 00 53 7f 00 00 00 00 30 07 53 7f 00 00 63 7f 28 02 64 7f 50 06 65 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 3b 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 3b 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.............{;w.............y ;w...............s................. {;w..........S.....0.S...c. (.d.P.e.................m........ ....`f;w.. ....PS;w.........B......	success or wait	11	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	5324	bc 9a 30 77 a3 1a 02 76 aa aa aa aa 68 ed 8b 02 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 f8 02 00 00 f4 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 50 b5 02 00 00 00 00 00 00 00 00 00 00 00 00 68 ed 8b 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..0w...v....h................ ....$.......... ....P ....h..............	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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 c8 ec 8b 02 bc 9a 30 77 23 00 00 00 02 02 00 00 38 eb 8b 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	?............................ ....+...S...+. ..+....................0...... ......0w#.......8...+.........	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	48	6c 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 10 b6 02 00 00 00 00 00 98 f7 6b 04 00 00 00 00 68 08 00 00 0c 53 00 00 cc 02 00 00 e4 2a 00 00	l....... ....k... ..h....S.......*..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.tmp.dmp	unknown	752	00 00 93 73 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 e0 41 02 00 00 00 00 00 10 d0 02 00 00 00 00 b4 4d 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 ca d9 00 00 00 00 00 00 27 4e 03 00 00 00 00 00 6d 96 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 dc e3 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b1 12 22 00 00 00 00	...s.....0...U..s@..2%.....B.....B?.....#.....@A.....Zb.....A.....A.....'N.....m.....!.....@....."....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4C3.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 c4 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 52 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.....`...R.....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.6.4.<./.P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 34 00 37 00 31 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.>.3.6.4.7.1.<./.U.p.t.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 35 00 36 00 38 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.>.1.2.7.8.1.5.6.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 36 00 39 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.>.2.6.9.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 36 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.6.6.8.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 36 00 36 00 38 00 34 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.>.9.1.6.6.8.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.8.4.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.5.7.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 38 00 39 00 33 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.8.9.3.4.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 39 00 31 00 38 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.1.8.7.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 38 00 39 00 33 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.8.9.3.4.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	28	3c 00 50 00 69 00 64 00 3e 00 32 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.0.4.<./.P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.6.7.8.2. <./.U.p.t.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 36 00 32 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.6.2.7.8.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 31 00 38 00 37 00 31 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.8.7.1.3.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 38 00 38 00 37 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.8.7.1.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 38 00 35 00 30 00 32 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.5.0.2.4.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.7.6.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.0.8.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 35 00 31 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.5.1.9.0.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 36 00 32 00 39 00 30 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.>.3.6.2.9.0.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 35 00 31 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.5.1.9.0.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 6b 00 6e 00 62 00 76 00 61 00 77 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.>.k.n.b.v.a.w.,. .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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 6b 00 6e 00 62 00 76 00 61 00 77 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.>.k.n.b.v.a.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 34 00 38 00 36 00 39 00 36 00 37 00 37 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.>.1.5.7.4.8.6.9.6.7.7.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 33 00 36 00 3a 00 31 00 32 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.:.3.6.:.1.2.Z.".>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 36 00 34 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 33 00 30 00 30 00 37 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 30 00 37 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.3.". .P.I.D.=.".5.4.6.4.". .U.p.t.i.m.e.M.S.=.".3.0.0.7.8.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.0.0.7.8.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 31 00 64 00 33 00 65 00 36 00 38 00 34 00 2d 00 65 00 32 00 36 00 66 00 2d 00 34 00 65 00 33 00 61 00 2d 00 38 00 65 00 34 00 31 00 2d 00 61 00 33 00 36 00 66 00 36 00 33 00 61 00 39 00 64 00 34 00 35 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.1.d.3.e.6.8.4.-.e.2.6.f.-.4.e.3.a.-.8.e.4.1.-.a.3.6.f.6.3.a.9.d.4.5.d.<./.G.u.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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 33 00 36 00 3a 00 31 00 32 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.:.3.6.:.1.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA14.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE5A.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367\Report.wer	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367\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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_6120cae27b7b1aa09340fa54c663327249d5f938_82810a17_18e2d367\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 36 00 35 00 36 00 30 00 33 00 39 00 31 00 32 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.6.5.6.0.3.9.1.2.2.	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D2636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D261FB2	RegCreateKeyExW
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D2636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{2e7e4d60-e5d5-67f9-7496-79a76e646ac3}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D2636BF	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	6D261FE8	RegSetValueExW

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

Disassembly

Code Analysis