ID: 413043
Sample Name:
87324661_by_Libranalysis
Cookbook: default.jbs
Time: 06:52:21
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 87324661_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
Malware Analysis System Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Authenticode Signature 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 15
Resources 16
Imports 16
Version Infos 16

Network Behavior 16
UDP Packets 16
Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: loaddll32.exe PID: 5424 Parent PID: 5708 18
General 18
File Activities 18
Analysis Process: cmd.exe PID: 5416 Parent PID: 5424 18
General 18
File Activities 19
Analysis Process: rundll32.exe PID: 1232 Parent PID: 5416 19
General 19
Analysis Process: WerFault.exe PID: 5384 Parent PID: 1232 19
General 19
File Activities 19
File Created 19
File Deleted 20
File Written 20
Registry Activities 42
Key Created 42
Key Value Created 42
Disassembly 43
Code Analysis 43

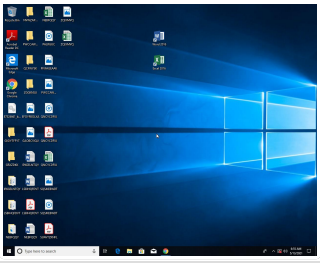
Analysis Report 87324661_by_Libranalysis

Overview

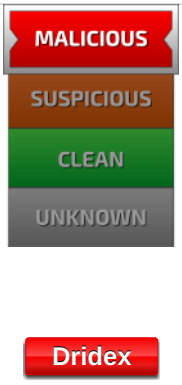
General Information

Sample Name:	87324661_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413043
MD5:	873246614925ee..
SHA1:	b92a017964f94fa..
SHA256:	78bad82ee02304..
Infos:	

Most interesting Screenshot:



Detection

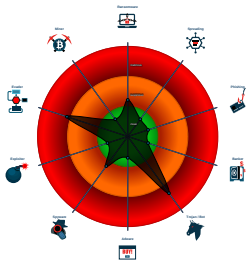


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes / dynamic…
- Antivirus or Machine Learning detec…
- 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…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5424 cmdline: loaddll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5416 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1232 cmdline: rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5384 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1232 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22202,
  "C2 list": [
    "203.114.109.124:443",
    "82.165.145.100:6601",
    "94.177.255.18:8172"
  ],
  "RC4 keys": [
    "BwjTiXD0nMT8wuL0lzuDMT1lwajgYLnSPMpMch1H2fk8H",
    "q9kldr5IysNmmZqCx9jFzlSDl8TYcZm1jGiJKdnQ5Lg6QzqUnZo1jkSGDQVP1"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000003.00000002.329383594.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

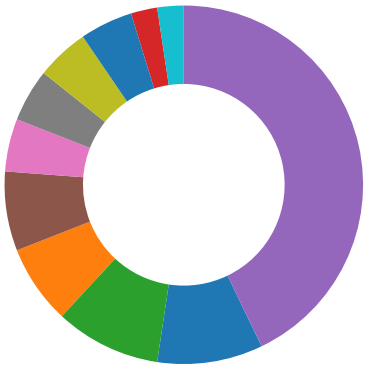
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.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

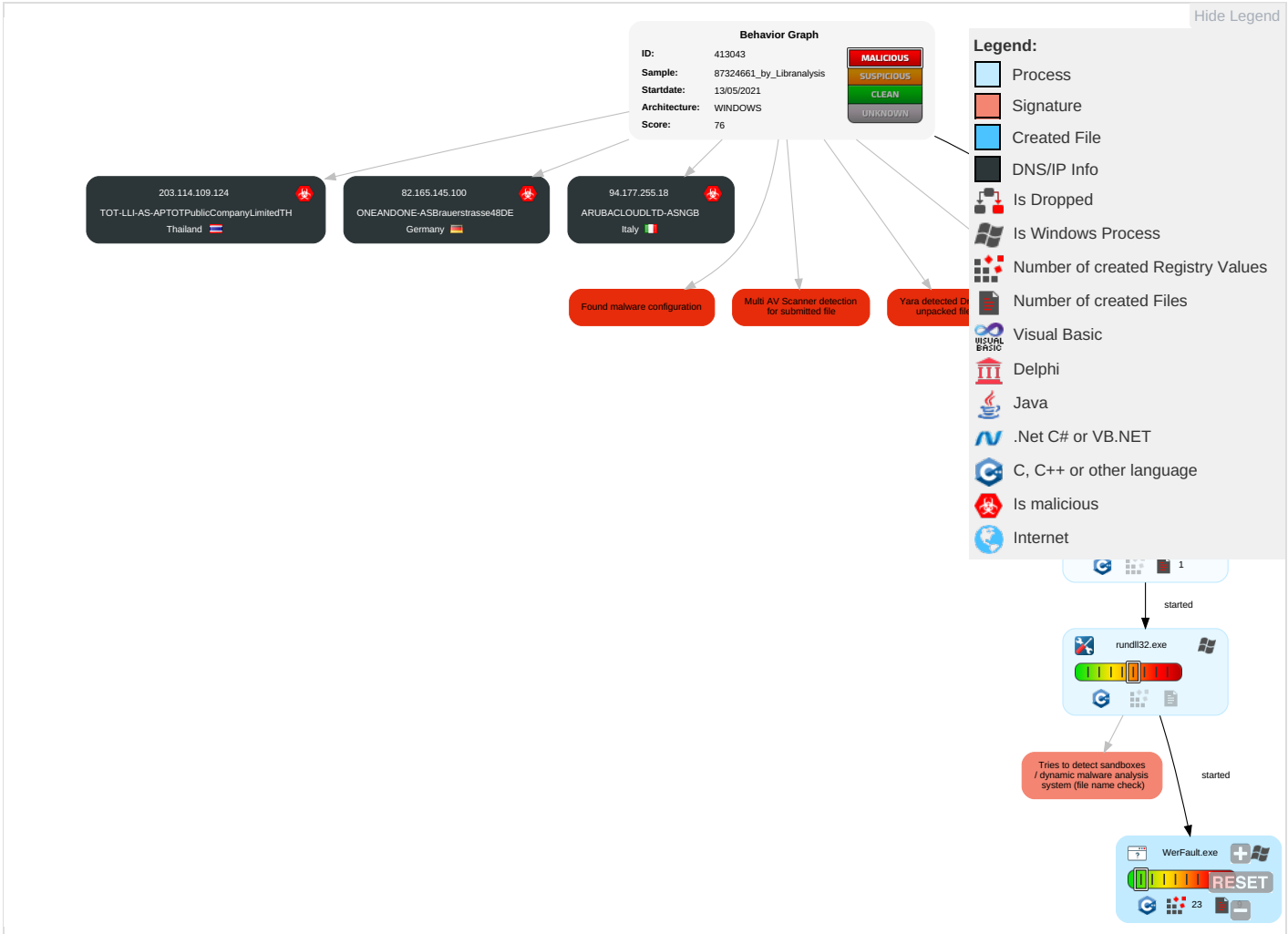
Malware Analysis System Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 1 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 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 3	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
87324661_by_Libranalysis.dll	68%	ReversingLabs	Win32.Infostealer.Dridex	
87324661_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.8e07fa.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.900000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	WerFault.exe, 00000010.0000000 2.325705287.0000000005130000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	WerFault.exe, 00000010.0000000 2.325705287.0000000005130000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	WerFault.exe, 00000010.0000000 2.325705287.0000000005130000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	WerFault.exe, 00000010.0000000 2.325705287.0000000005130000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413043
Start date:	13.05.2021
Start time:	06:52:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	87324661_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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.1% (good quality ratio 50.1%) • Quality average: 67% • Quality standard deviation: 35.5%
HCA Information:	• Successful, ratio: 71% • 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
06:53:53	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
94.177.255.18	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
203.114.109.124	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 94.177.255.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12688
Entropy (8bit):	3.76777862063572
Encrypted:	false
SSDEEP:	192:x+6iM0oXprYRHBUZMX4jed+0YwR/u7saS274ItWck:U6iKXVWBUZMX4jeb7/u7saX4ItWck
MD5:	1256256EA6A39E799376E56238EC9099
SHA1:	14D1CC8EE890E72F193982A08A9044A3EE8E4019
SHA-256:	28342B0B2EFEBB88CF401D5D7A6C4028F4E560FD2647470CBC5FBD2F99FE017C
SHA-512:	FF14D76D186E2D97D9EF3794A12587EF99561E3E8D57F5DBCB71C8429687C96C045CEF3AD8BB68441FD0F1C74AE583149858551041894E30434DC9CF1B225E9
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.7.6.2.6.1.1.8.7.2.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.7.6.3.1.4.1.5.5.8.3.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.8.a.1.0.b.8.0.-.1.c.a.4.-.4.4.7.9.-.a.7.7.e.-.8.5.4.a.8.6.1.9.7.e.1.c.....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.=.7.0.0.5.8.2.a.c.-.8.a.e.7.-.4.3.e.1.-.8.3.0.a.-.b.d.4.7.c.e.1.4.a.1.2.8.....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.=.0.0.0.0.0.0.4.d.0.-.0.0.0.1.-.0.0.1.7.-.3.e.e.a.-.9.4.4.f.f.f.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:53:47 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40860
Entropy (8bit):	2.4130070038902205
Encrypted:	false
SSDEEP:	192:pb8Z42iljusSocgMEU7G3aLDc4YQ9aP1LdyD8PhR:S3LmGeA4Hu1LdyDGR
MD5:	C063AFF7BDFA3074088905422B00388D
SHA1:	AA47847CFB6B72D4E012F13EB1203068A57477F3
SHA-256:	81039B7FFA0E0FDE21D0CD0A9B0885F69889FB64CBE2685F1C12D7211BEEBADB
SHA-512:	7E52A69AE88F2EACFD2BC493976044B28DBFF35B773E9506F6F0755AB9E4928BAA712BE518449C74DB0341ED773F7743B6A1885208CEDE225EAE7040B0CC61D5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....k/.`.....U.....B.....P .....GenuineIntelW.....T.....F/.`.....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\WERA7D4.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

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	
Size (bytes):	8292
Entropy (8bit):	3.692604650550988
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivo6nQQ06YNV6egKGgmfTUYuSVCprf89bMnZCsfLEm:RrlsNiw6c6Y/6eEgmfTU/SNMnZBft
MD5:	788C5E2F33ED0137284CAB89A44F043F
SHA1:	8B2C4CF539F36D75DD888800665C2CF9CC8D85E0
SHA-256:	24EBCB636C8C1D25399070350AC2C8BECAE0573A65CA27AAAC7442109F07754E
SHA-512:	9B09F15D2847FBB5766CC6EE57A0C7B8D30206E6FDFBC1E345AB05A3AD8E3558DCE6785C8229E221604ECE49B4499D81151ED04DE46C43462F7F9740CFC674
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.>.1.2.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.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):	4.472044710158667
Encrypted:	false
SSDEEP:	48:cvIwSD8zshrJgtWI9ESWSC8Bz8fm8M4JCdsDNCFQI+q8/KNFwi54SrSVd:uITfD3zSNOJBNZIxNmi5DWVd
MD5:	27E573A2A68D586CF24B3916F9CDB96F
SHA1:	B6156BF3D6FB3EC1F5DC520C9B7317B4D6EB8504
SHA-256:	93DF4769AFAD409511CD849738658BDBE0BF28602E87A3D82A418EC92CC80219
SHA-512:	47062DEEB539F15EF6C7192667A5DCB7C7209E5685CEF7A0B6DF7FBC56478B3EE0176038320E216EA12E932C96729FF80A2C6130EF7C667A82713B0CC1B3619(
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="987784" />.. <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):	7.585730266072232
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:	87324661_by_Libranalysis.dll
File size:	166856
MD5:	873246614925eed7eb818ffa6f785b75
SHA1:	b92a017964f94fa7cf2c77a95ea1095513c5431d
SHA256:	78bad82ee0230454a48cc41c1a951c304027ffc7d1b5d2c1b5bc4567db455109
SHA512:	92bca7ae32d548dfaaae3ae78de2f07d7dca1b43fc1039fd32a6a751662d4e3a8b7b2d56577d1c18b64d4b7d286f7025dfdc9787706c8cf100f339fc61e55013
SSDEEP:	3072:besl4+VdlY+01jb5SA5hg9PTEfPa1x+pq0KbuFicLiV:f4+VZQpt5hyPsa1ekiE9V
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.%.0zK.0zK.0zK.0zJ.}{K...3..{K.....P{K...3..zK.V....zK...1..{K.....zK.Rich0zK.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10023140
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F8E [Thu May 13 01:23:26 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:	a86a1220a8aaf2bed0594d018b59c83f

Authenticode Signature

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

Entrypoint Preview

Instruction
xor eax, eax
add eax, 00002234h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
jne 00007F96248A1E29h
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
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] VS2012 UPD3 build 60610 • [LNK] VS2005 build 50727 • [EXP] VS2005 build 50727 • [C] VS2012 UPD4 build 61030 • [IMP] VS2013 UPD2 build 30501

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x222bc	0x22400	False	0.76244582573	data	7.58615299723	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x2a76	0x2c00	False	0.787819602273	SysEx File -	7.46416514998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x27000	0x3307	0x1800	False	0.76806640625	MMDF mailbox	7.41456160551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x3a0	0x400	False	0.423828125	data	3.05991849143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x2c000	0x230	0x400	False	0.4951171875	data	3.95131264834	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
ADVAPI32.dll	RegOverridePredefKey
CLUSAPI.dll	ClusterEnum
RASAPI32.dll	RasGetConnectionStatistics
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
OPENGL32.dll	glTexSubImage1D
KERNEL32.dll	CloseHandle, LoadLibraryExA, OutputDebugStringA, CreateFileW, GetProfileSectionW, GetProfileSectionA, LoadLibraryW, OpenSemaphoreW
USER32.dll	TranslateMessage

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

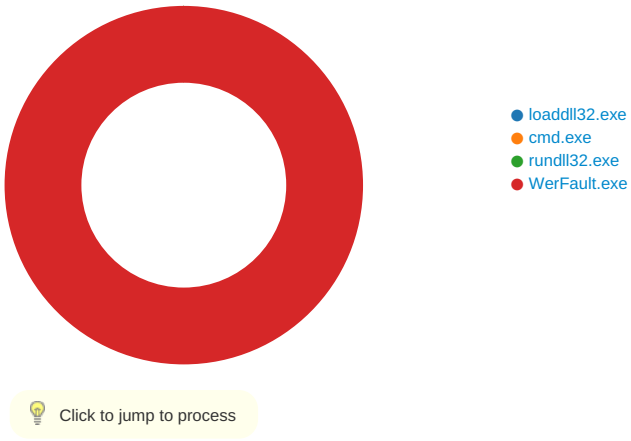
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:53:03.650938988 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 06:53:04.575496912 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:04.636465073 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 06:53:05.169647932 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:05.220032930 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 06:53:06.270973921 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:06.322563887 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 06:53:07.190846920 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:07.241010904 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 06:53:08.213059902 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:08.270248890 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 06:53:10.013606071 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:10.062330961 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 06:53:10.982935905 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:11.042082071 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 06:53:12.093765974 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:12.150939941 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 06:53:15.986905098 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:16.040357113 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 06:53:17.299525976 CEST	54008	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:53:17.356952906 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 06:53:18.371773958 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:18.422003984 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 06:53:19.375796080 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:19.425734997 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 06:53:20.320971012 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:20.379380941 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 06:53:22.141390085 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:22.190107107 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 06:53:23.126115084 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:23.177876949 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 06:53:24.430749893 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:24.479428053 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 06:53:29.998092890 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:30.058737993 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 06:53:31.377778053 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:31.428180933 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 06:53:32.585802078 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:32.634721994 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 06:53:34.213552952 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:34.262284040 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 06:53:35.594146967 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:35.642837048 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 06:53:38.883027077 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:38.931754112 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 06:53:40.004771948 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:40.055289030 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 06:53:50.918724060 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:50.993432999 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 06:53:53.093300104 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:53.142174959 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 06:53:59.845599890 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:53:59.909684896 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 06:54:08.344572067 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 06:54:08.403266907 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 06:54:33.806541920 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 06:54:33.871860027 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 06:54:44.187128067 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 06:54:44.245999098 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 06:54:59.335824966 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 06:54:59.449593067 CEST	53	56064	8.8.8.8	192.168.2.7
May 13, 2021 06:54:59.995862961 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:00.055728912 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 06:55:00.476495028 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:00.548268080 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 06:55:00.685201883 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:00.750860929 CEST	53	58367	8.8.8.8	192.168.2.7
May 13, 2021 06:55:01.225806952 CEST	60599	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:01.283047915 CEST	53	60599	8.8.8.8	192.168.2.7
May 13, 2021 06:55:01.842647076 CEST	59571	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:01.902240038 CEST	53	59571	8.8.8.8	192.168.2.7
May 13, 2021 06:55:02.463356972 CEST	52689	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:02.522622108 CEST	53	52689	8.8.8.8	192.168.2.7
May 13, 2021 06:55:03.004291058 CEST	50290	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:03.067368984 CEST	53	50290	8.8.8.8	192.168.2.7
May 13, 2021 06:55:03.937666893 CEST	60427	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:03.997759104 CEST	53	60427	8.8.8.8	192.168.2.7
May 13, 2021 06:55:05.019449949 CEST	56209	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:05.077378035 CEST	53	56209	8.8.8.8	192.168.2.7
May 13, 2021 06:55:05.508192062 CEST	59582	53	192.168.2.7	8.8.8.8
May 13, 2021 06:55:05.625802040 CEST	53	59582	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5424 Parent PID: 5708

General

Start time:	06:53:10
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll'
Imagebase:	0x1050000
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: 5416 Parent PID: 5424

General

Start time:	06:53:10
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\87324661_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: 1232 Parent PID: 5416

General

Start time:	06:53:10
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1
Imagebase:	0xe00000
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: 00000003.00000002.329383594.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5384 Parent PID: 1232

General

Start time:	06:53:43
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1232 -s 764
Imagebase:	0x1240000
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

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	6D071717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D06497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.tmp	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	success or wait	1	6D064BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	success or wait	1	6D064BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.tmp.xml	success or wait	1	6D064BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA92.tmp.csv	success or wait	1	6D064BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAEE8.tmp.txt	success or wait	1	6D064BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 6b 2f 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....k/.`.....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.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 50 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 d0 04 00 00 46 2f 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 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......P .... ..GenuineIntelW...........T... ....F/.`.................. ....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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 d0 50 00 10 c0 36 af 00 ff ff ff ff d0 50 00 10 fa 0a 00 02 d4 f6 56 00 d5 50 00 10 23 00 00 00 86 02 01 00 50 f6 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........P...6.......P...... ..V..P..#.......P.V.+.........	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	168	d0 17 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 d5 50 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 8b 1f f3 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a 26 00 00	........................P.... ....Z&..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	20	0c 00 00 00 54 e6 56 00 00 00 00 00 ac 19 00 00 82 2f 00 00	....T.V........../..	success or wait	12	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	6572	bc 9a 30 77 a3 1a 02 76 aa aa aa aa 88 e8 56 00 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 aa aa aa aa 00 f0 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 88 e8 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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......V.............. ....$........... ....V............	success or wait	11	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	4	74 68 65 6d	them	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa d0 50 00 10 00 00 00 00 e8 e7 56 00 bc 9a 30 77 23 00 00 00 02 02 00 00 58 e6 56 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+....................P...... ..V...0w#.......X.V.+.........	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	48	44 05 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 e0 60 00 00 00 00 00 54 fb da 00 00 00 00 00 ac 04 00 00 d2 6f 00 00 cc 02 00 00 f2 2b 00 00	D....... ....`.....T..... ....o.......+..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	53	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	752	00 00 7a 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 40 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 e0 30 02 00 00 00 00 00 10 df 02 00 00 00 00 17 50 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 02 ca 00 00 00 00 00 00 92 51 03 00 00 00 00 00 39 a4 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 d1 e5 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 bb f8 21 00 00 00 00	..zs.....0...U..s@..@&.....B.....B?.....#.....@A.....Zb.....0.....P.....Q.....9.....!.....@.....!....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.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	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA09F.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 be 2e 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 84 81 00 00 15 00 00 00 ec 01 00 00 cc 1d 00 00 16 00 00 00 98 00 00 00 b8 1f 00 00	....d.....`...l..... .....T.....8..... ....T.....`.....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 32 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.2.3.2.<./.P.i.d.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 37 00 31 00 39 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.7.1.9.8.<./.U.p.t.i.m.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 38 00 33 00 31 00 31 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.1.1.2.9.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 38 00 33 00 30 00 33 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.>.1.2.8.3.0.3.1.0.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 37 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.7.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 31 00 36 00 37 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.>.9.4.1.6.7.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 31 00 36 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.1.6.7.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.8.7.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 32 00 38 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 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.2.8.0.<./.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 30 00 30 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.>.3.1.0.0.8.<./.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 38 00 35 00 39 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.8.5.9.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 34 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.9.4.1.4.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 38 00 35 00 39 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.8.5.9.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.1.6.<./.P.i.d.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 37 00 35 00 39 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.>.3.7.5.9.1. <./.U.p.t.i.m.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 31 00 32 00 39 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.2.9.7.9.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 30 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.>.1.1.2.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 33 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.1.4.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 34 00 35 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.4.5.9.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.5.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 31 00 31 00 30 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.>.2.3.5.1.1.0.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 30 00 34 00 34 00 38 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.>.3.6.0.4.4.8.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 31 00 31 00 30 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.>.2.3.5.1.1.0.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 64 00 69 00 6f 00 6e 00 6e 00 73 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.>.d.i.o.n.n.s.,. .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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 64 00 69 00 6f 00 6e 00 6e 00 73 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.>.d.i.o.n.n.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 36 00 37 00 39 00 30 00 38 00 38 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.6.7.9.0.8.8.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 33 00 3a 00 34 00 38 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.3.:.5.3.:.4.8.Z.".>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 32 00 33 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 31 00 39 00 32 00 31 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 31 00 39 00 32 00 31 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.=.".3.3.6.". .P.I.D.=.".1.2.3.2.". .U.p.t.i.m.e.M.S.=.".3.1.9.2.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.1.9.2.1.". .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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 38 00 61 00 31 00 30 00 62 00 38 00 30 00 2d 00 31 00 63 00 61 00 34 00 2d 00 34 00 34 00 37 00 39 00 2d 00 61 00 37 00 37 00 65 00 2d 00 38 00 35 00 34 00 61 00 38 00 36 00 31 00 39 00 37 00 65 00 31 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.8.a.1.0.b.8.0.-.1.c.a.4.-.4.4.7.9.-.a.7.7.e.-.8.5.4.a.8.6.1.9.7.e.1.c.<./.G.u.i.d.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 33 00 3a 00 34 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:.5.3.:.4.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7D4.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	6D06497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA65.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	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d\Report.wer	unknown	2	ff fe	..	success or wait	1	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	184	6D06497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_154bbd7d\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 32 00 30 00 34 00 35 00 36 00 30 00 33 00 32 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.2.0.4.5.6.0.3.2.9.	success or wait	1	6D06497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D0836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D081FB2	RegCreateKeyExW
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D0643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D0836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D0836BF	unknown
\REGISTRY\A\{d13c3f16-55b0-c8eb-ce16-6e81bf032c86}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D0836BF	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 D5 50 00 10 02 00 00 00 01 00 00 00 8B 1F F3 7F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D081FE8	RegSetValueExW

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

Disassembly

Code Analysis