

JOeSandbox Cloud BASIC



ID: 413046

Sample Name:

042529de_by_Libranalysis

Cookbook: default.jbs

Time: 06:56:23

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 042529de_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	16
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: 4844 Parent PID: 5704	18
General	18
File Activities	19
Analysis Process: cmd.exe PID: 2236 Parent PID: 4844	19
General	19
File Activities	19
Analysis Process: rundll32.exe PID: 1008 Parent PID: 2236	19
General	19
Analysis Process: WerFault.exe PID: 7008 Parent PID: 1008	19
General	20
File Activities	20
File Created	20
File Deleted	20
File Written	20
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 042529de_by_Libranalysis

Overview

General Information

Sample Name:

042529de_by_Libranalysis
(renamed file extension from none to dll)

Analysis ID:

413046

MD5:

042529de19df790.

SHA1:

f9f73e973dda28b..

SHA256:

430143aaf388f90..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Tries to detect sandboxes / dynamic...

Checks if the current process is bein...

Contains functionality to check if a d...

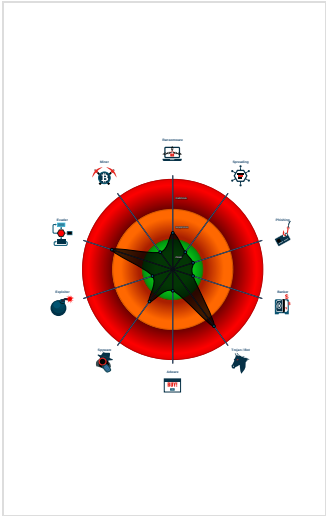
Contains functionality to query locale...

Creates a DirectInput object (often fo...

Creates a process in suspended mo...

Detected potential crypto function

Classification



Startup

System is w10x64

loadaddll32.exe (PID: 4844 cmdline: loadaddll32.exe 'C:\Users\user\Desktop\042529de_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 2236 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\042529de_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 1008 cmdline: rundll32.exe 'C:\Users\user\Desktop\042529de_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 7008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1008 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 22201,
  "C2 list": [
    "203.114.109.124:443",
    "82.165.145.100:6601",
    "94.177.255.18:8172"
  ],
  "RC4 keys": [
    "BwjTtX00nMT8wuL0LzuDMT1lwaJgYLnSPMpMch1H2fk8H",
    "Zn2kewZLGvQs4cF0q75iWd3gnwzXSWs561WqaqBWjN3RtNQtcvkRtchJba3Ed"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.330690935.0000000010001000.0000020.00020000.sdmf	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

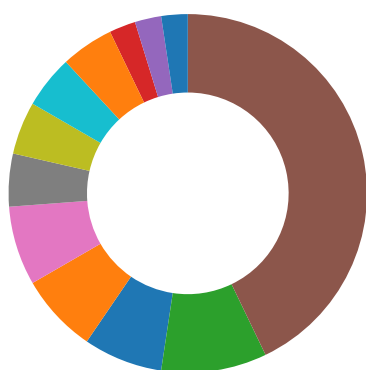
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



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

💡 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Dridex unpacked file

Malware Analysis System Evasion:

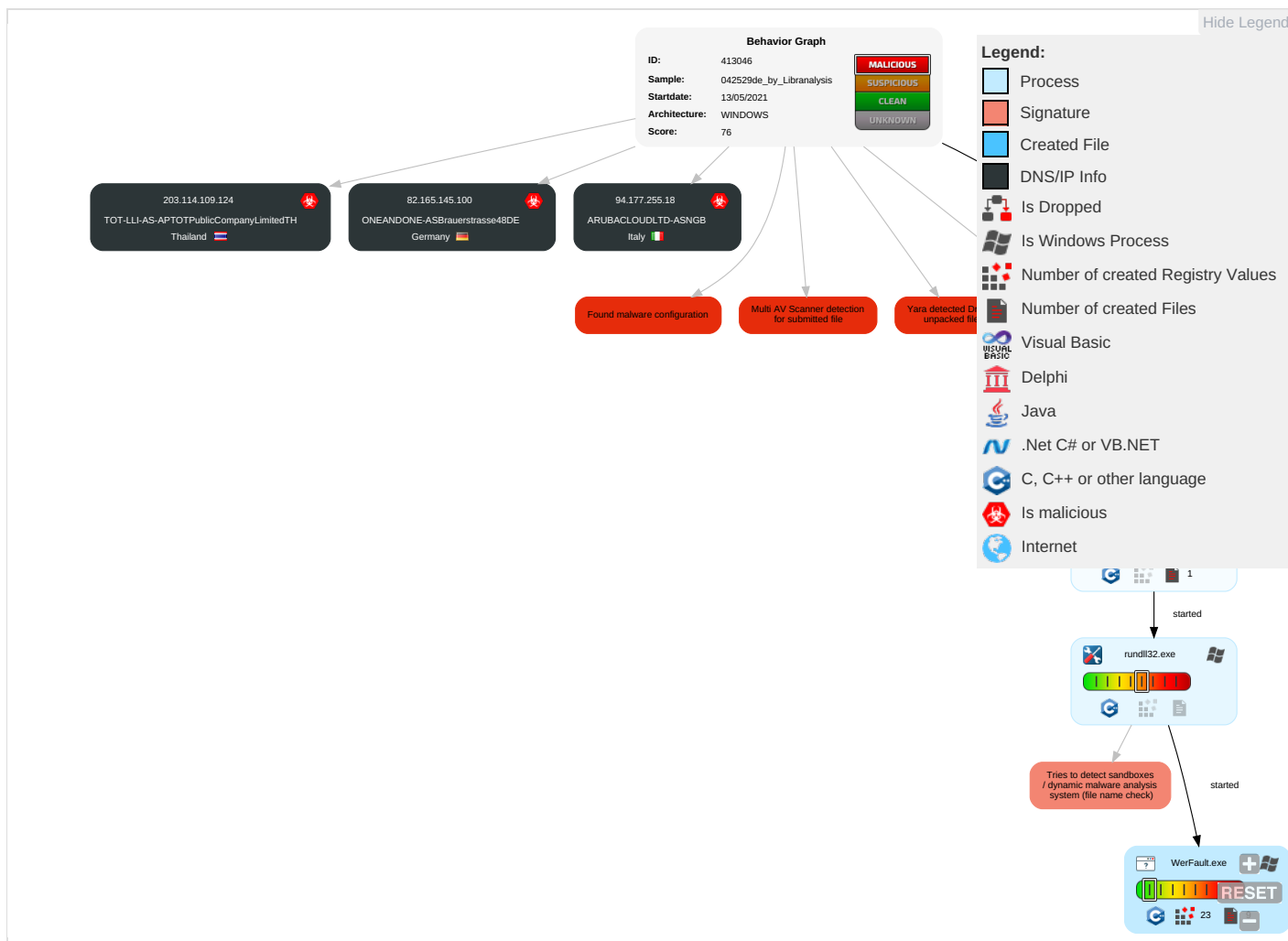


Tries to detect sandboxes / dynamic malware analysis system (file name check)

Mitre Att&ck Matrix

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

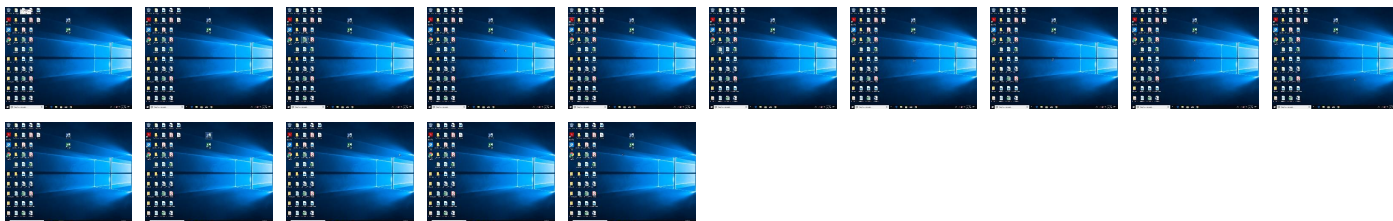
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
042529de_by_Libranalysis.dll	62%	ReversingLabs	Win32.Infostealer.Dridex	
042529de_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.4e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	WerFault.exe, 0000000F.000000002.328387581.0000000005800000.00000002.00000001.sdmp, 042529de_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	WerFault.exe, 0000000F.000000002.328387581.0000000005800000.00000002.00000001.sdmp, 042529de_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://ocsp.sectigo.com0	WerFault.exe, 0000000F.000000002.328387581.0000000005800000.00000002.00000001.sdmp, 042529de_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, 0000000F.000000002.328387581.0000000005800000.00000002.00000001.sdmp, 042529de_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-ASBraucherstrasse48DE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413046
Start date:	13.05.2021
Start time:	06:56:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	042529de_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:	30
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: 94.2% (good quality ratio 84.8%) - Quality average: 71.1% - Quality standard deviation: 33%
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
06:57:58	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	87324661_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	
203.114.109.124	87324661_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBraucherstrasse48DE	87324661_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
TOT-LLI-AS-APTOTPublicCompanyLimitedTH	87324661_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
ARUBACLOUDLTD-ASNGB	87324661_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
	931f389a_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	ed938820_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	ab44ae30_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	e442fdd8_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	8ca7a263_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	2617efd0_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	ec120f08_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	83832e74_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	cce7d578_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	be825cf1_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12684
Entropy (8bit):	3.7675682588990025
Encrypted:	false
SSDEEP:	192:S/ir0oXTGiYHBUZMX4jed+bwR/u7s2S274ltWcy:Si1XTkBUZMX4jeV/u7s2X4ltWcy
MD5:	CF4C7262591EEB77CC497704042A3006
SHA1:	F1C344130C7169F7722BF741427A629960EA0859
SHA-256:	945D8FB97A3B01C69084F26F4C038EEC854BC12E4853D08E7A8F1597F705F5A6
SHA-512:	E9957FD17F6D8382F63D51F45DC3E9DE8B461472A959141154D5D6974C6479C90931C0FB598D8B11BF2784B74FD504F29C5B02D762EF0716785E2EC1A3EA8D9
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.=1.3.2.6.5.3.8.7.8.6.8.5.8.8.8.3.3.6.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.2.6.5.3.8.7.8.7.6.1.9.8.1.8.6.1.....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.=a.d.8.d.c.d.9.8.-6.3.8.2.-4.e.c.3.-b.d.d.a.-5.5.3.2.1.9.b.6.d.0.d.8.....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.=9.b.a.6.e.5.8.4.-b.e.1.3.-4.8.0.8.-b.2.4.1.-e.c.3.d.9.f.e.9.5.f.d.f.....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.=0.0.0.0.0.3.f.0.-0.0.0.1.-0.0.1.7.-c.d.d.a.-e.b.d.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\WER1E97.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:57:50 2021, 0x1205a4 type
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp.dmp	
Size (bytes):	40932
Entropy (8bit):	2.3894657397967505
Encrypted:	false
SSDEEP:	192:/NdFbhhpPjZq4YszocqMEU7G3aLTcRro3JNqZluYfE:fRpH9geT6rONqZ/fe
MD5:	D0531B75E056E6E769887CADB931B07A
SHA1:	A3A471094FD64D7C844FF5CF4E2703074632537C
SHA-256:	AA51272E58FDD0AF8A607C118F95C9662999DFBDE7A4CED269F7F64595991AA2
SHA-512:	7CB30B87D146C4C44AF71603456924DEF0343C3BA5A05F9A983917DF23295CBC1C8F484D50492B4945F6374CAB356F08A33BD76BD6632233EDF418EF31D25D9F
Malicious:	false
Reputation:	low
Preview:	MDMP.....^0`.....U.....B.....P.....GenuineIntelW.....T.....80.`.....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\WER2734.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8292
Entropy (8bit):	3.6938064463575477
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMvY6nG6YWo6VSgmft7ZSUCprv89bwwnGsf0P92m:RrlsNiM66G6YB6VSgmfTtSMwnlfG/
MD5:	7289C8F390F18CC6BCCADFF6E9E6A7CC
SHA1:	FE84CB5CE8317083554A39DAC5EE6FE6964A87BC
SHA-256:	614F200D0C19E649508BA613E34292DE1CDF6701E736399777D15FFBA755346F
SHA-512:	FF36077BAD3F5C0523D59A702C08DF163BF31177E8D4E6F53F3F5B012A768268EE3E67CF329D5B02D9C064E8DEE7C2A6FA2ECAD87272D6FF753C1893BB25311
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.>1.0.0.8<./P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.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):	4.4742919696922865
Encrypted:	false
SSDEEP:	48:cvlwSD8zsVjgtWi9EqWSC8Bg8fm8M4JCds/bNntF3m+q8/MbNFnL4SrS41d:ulTfvTLsNzJNbNe9bNFDWCd
MD5:	E3378408341C99A0B0A96CADB5084621
SHA1:	12B6643E54A3D838501A9E7A84C47E46EF6D17E1
SHA-256:	98AF9C3CA1151C915C9ABFE9A15B82C499AD548C37A34F7AF06585185672AD45
SHA-512:	EDBE410A76B86C846B82CDB3A315B19ECB788921FED0BB865821A41B95C6E6EE4922E972C8206A990F01109B2B7E49AA9EA3C9B0D6F3C67E4185BC43D1B583D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">..<tlm>..<src>..<desc>..<mach>..<os>..<arg nm="vermaj" val="10" />..<arg nm="vermin" val="0" />..<arg nm="verblid" val="17134" />..<arg nm="vercsdbld" val="1" />..<arg nm="verqfe" val="1" />..<arg nm="csdbld" val="1" />..<arg nm="versp" val="0" />..<arg nm="arch" val="9" />..<arg nm="lcid" val="1033" />..<arg nm="geoid" val="244" />..<arg nm="sku" val="48" />..<arg nm="domain" val="0" />..<arg nm="prodsuite" val="256" />..<arg nm="ntprodtype" val="1" />..<arg nm="platid" val="2" />..<arg nm="tmsi" val="987788" />..<arg nm="osinsty" val="1" />..<arg nm="iever" val="11.1.17134.0-1.0.47" />..<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

General

Entropy (8bit):	7.583613798367438
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:	042529de_by_Libranalysis.dll
File size:	166856
MD5:	042529de19df790cdf8fe1a26ae1d5aa
SHA1:	f9f73e973dda28b2b82fc3c3bb5f0740f6d28ea1
SHA256:	430143aaf388f90ce6766480df547460ed3588347b4c58871accd32fa8a0961b
SHA512:	73381bf28bca8a5cca1f9675a13fd9d57ad9a004626e4d5e016efb614b95cb9768010fad774c56d738ddb75aa75c7c07f6f5d5a1d9e75bc3bc31df17f4db37e4
SSDEEP:	3072:F/FbrEzD9N+RiMB00c9/74DXE+JgaV7IPx+e6O/pPtaLOi:3brE1kvcB74DXZ2Mel3i
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......t.%0zK. 0zK.0zK.0zJ.){K...3..{K.....P{K...3..zK.V...zK...1..{K.....z K.Rich0zK.....PE..L..

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10023130
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F93 [Thu May 13 01:23:31 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:	35893a758d71a4b313745582f88cf6b6

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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Resources

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

Imports

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

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:57:05.497380972 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:05.554747105 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 06:57:06.027421951 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:06.084467888 CEST	53	60501	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:57:06.247921944 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:06.296725035 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 06:57:07.329972982 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:07.381485939 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 06:57:08.530333996 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:08.579020023 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 06:57:09.923357010 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:09.960467100 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:09.972031116 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 06:57:10.024082899 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 06:57:11.531532049 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:11.588655949 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 06:57:12.667609930 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:12.716346979 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 06:57:14.364583969 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:14.421838999 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 06:57:22.150432110 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:22.199636936 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 06:57:23.267908096 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:23.325012922 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 06:57:25.443334103 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:25.494931936 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 06:57:26.485157013 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:26.534009933 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 06:57:33.341187954 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:33.400007963 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 06:57:34.791951895 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:34.840886116 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 06:57:35.913252115 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:35.962047100 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 06:57:37.069798946 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:37.118942022 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 06:57:38.813409090 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:38.865058899 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 06:57:40.074878931 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:40.123526096 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 06:57:41.307329893 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:41.357032061 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 06:57:42.836102962 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:42.884879112 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 06:57:43.990967989 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:44.040106058 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 06:57:44.942949057 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:44.994451046 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 06:57:47.105863094 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:47.154968977 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 06:57:56.365051031 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:56.440208912 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 06:57:57.532074928 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 06:57:57.589720964 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 06:58:01.251290083 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 06:58:01.312550068 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 06:58:02.474287033 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 06:58:02.523000002 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 06:58:11.694286108 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:58:11.754353046 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 06:58:42.742275953 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 06:58:42.808885098 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 06:58:48.056348085 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 06:58:48.124034882 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 06:59:03.320688963 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:03.426789045 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 06:59:04.068598032 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:04.170871019 CEST	53	56064	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:59:04.491632938 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:04.562212944 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 06:59:04.791532993 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:04.848692894 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 06:59:05.337626934 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:05.401299953 CEST	53	58367	8.8.8.8	192.168.2.7
May 13, 2021 06:59:06.034526110 CEST	60599	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:06.091675997 CEST	53	60599	8.8.8.8	192.168.2.7
May 13, 2021 06:59:06.724257946 CEST	59571	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:06.783740044 CEST	53	59571	8.8.8.8	192.168.2.7
May 13, 2021 06:59:07.289761066 CEST	52689	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:07.346870899 CEST	53	52689	8.8.8.8	192.168.2.7
May 13, 2021 06:59:08.170528889 CEST	50290	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:08.233360052 CEST	53	50290	8.8.8.8	192.168.2.7
May 13, 2021 06:59:09.265723944 CEST	60427	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:09.325908899 CEST	53	60427	8.8.8.8	192.168.2.7
May 13, 2021 06:59:09.943453074 CEST	56209	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:10.000729084 CEST	53	56209	8.8.8.8	192.168.2.7
May 13, 2021 06:59:18.568387985 CEST	59582	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:18.626960993 CEST	53	59582	8.8.8.8	192.168.2.7
May 13, 2021 06:59:19.479314089 CEST	60949	53	192.168.2.7	8.8.8.8
May 13, 2021 06:59:19.536600113 CEST	53	60949	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



- loadll32.exe
- cmd.exe
- rundll32.exe
- WerFault.exe

Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 4844 Parent PID: 5704

General

Start time:	06:57:12
Start date:	13/05/2021

Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\042529de_by_Libranalysis.dll'
Imagebase:	0xb20000
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: 2236 Parent PID: 4844

General

Start time:	06:57:12
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\042529de_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: 1008 Parent PID: 2236

General

Start time:	06:57:12
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\042529de_by_Libranalysis.dll',#1
Imagebase:	0xc50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.330690935.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 7008 Parent PID: 1008

General

Start time:	06:57:44
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1008 -s 764
Imagebase:	0x1070000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CB51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CB4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.tmp	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp.dmp	success or wait	1	6CB44BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	success or wait	1	6CB44BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.tmp.xml	success or wait	1	6CB44BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AAD.tmp.csv	success or wait	1	6CB44BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E29.tmp.txt	success or wait	1	6CB44BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp.dmp	unknown	752	00 00 93 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 00 00 23 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 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 20 31 02 00 00 00 00 00 30 e7 02 00 00 00 00 1d 4f 01 00 00 01 00 00 00 00 00 00 ff ff ff 00 00 00 00 44 d7 00 00 00 00 00 00 82 4f 03 00 00 00 00 00 60 9a 02 00 00 00 00 00 ff ff ff 00 00 00 00 0b ef 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 7d 26 22 00 00 00 00	...S.....0...U..s@..@&.....B.....B?.....#..... ..@A.....Zb..... 1.....0..... .O.....D.....O`.....! @.....}&".....	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	E.v.e.n.t.....F.i.l.e.....F.i.l.e.. (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.I.R.T.i.m	success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E97.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 cc 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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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.-16"?>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 30 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.0.0.8.<./P.i.d.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 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.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 38 00 36 00 36 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.>.3.7.8.6.6.<./U.p.t.i.m.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.l.p.t.E.n.a.b.l.e.d.>.0.<./l.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.6.6.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 33 00 39 00 32 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.3.9.2.1.2.8.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 33 00 39 00 32 00 31 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 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.>.9.3.9.2.1.2.8.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.1.8.6.4.4.8.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 33 00 34 00 34 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>.3.1.3.4.4.<./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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 37 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 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>.3.1.0.7.2.<./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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 39 00 30 00 30 00 34 00 38 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>.5.8.9.0.0.4.8.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 38 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.9.8.2.4.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 39 00 30 00 30 00 34 00 38 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.>.5.8.9.0.0.4.8.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 32 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.2.3.6.<./P.i.d.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 32 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e>.3.8.2.9.4.<./U.p.t.i.m.e>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.l.p.t.E.n.a.b.l.e.d>.0.<./l.p.t.E.n.a.b.l.e.d>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 33 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.>.1.1.2.3.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 31 00 36 00 37 00 36 00 38 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.>.3.6.1.6.7.6.8.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 3e 00	<./P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 61 00 6f 00 70 00 74 00 79 00 74 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.a.o.p.t.y.t.,.I.n.c...<./S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 61 00 6f 00 70 00 74 00 79 00 74 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.a.o.p.t.y.t.7,..1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 35 00 39 00 33 00 39 00 38 00 30 00 31 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>.1.5.5.9.3.9.8.0.1.6.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.<./F.l.a.g.s.>.	success or wait	3	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 37 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-.0.5.-.1.3.T.1.3.:.5.7.: 5.1.Z.">.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 30 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 30 00 35 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 35 00 31 00 35 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 33 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.= ".3.3.7.". .P.I.D.= ".1.0.0.8". .U.p.t.i.m.e.M.S.= ".3.0.5.1.5". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".3.0.5.1.5". .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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 64 00 38 00 64 00 63 00 64 00 39 00 38 00 2d 00 36 00 33 00 38 00 32 00 2d 00 34 00 65 00 63 00 33 00 2d 00 62 00 64 00 64 00 61 00 2d 00 35 00 35 00 33 00 32 00 31 00 39 00 62 00 36 00 64 00 30 00 64 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.d.8.d.c.d.9.8-.6.3.8.2.-.4.e.c.3.-.b.d.d.a-.5.5.3.2.1.9.b.6.d.0.d.8.<./G.u.i.d.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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 37 00 3a 00 35 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:5.7.:5.1.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2734.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	6CB4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A90.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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450\Report.wer	unknown	2	ff fe	..	success or wait	1	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450\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	6CB4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_b9c383acf725d24c7ce2a6d77f1a2161252591c_82810a17_1b214450\Report.wer	unknown	44	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 36 00 39 00 35 00 36 00 32 00 32 00 30 00 36 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.6. 9.5.6.2.2.0.6.9.	success or wait	1	6CB4497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB636BF	unknown
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB636BF	unknown
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	success or wait	1	6CB636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CB61FB2	RegCreateKeyExW
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	6CB636BF	unknown
\REGISTRYA\{8dadbfdf-045b-774f-79be-0121fbb8eb1f}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CB636BF	unknown

