

JOeSandbox Cloud BASIC



ID: 413043

Sample Name:

87324661_by_Libranalysis.dll

Cookbook: default.jbs

Time: 06:59:59

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 87324661_by_Libranalysis.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Malware Analysis System Evasion:	5
Mitre Att&ck Matrix	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	14
General	14
File Icon	14
Static PE Info	14
General	14
Authenticode Signature	15
Entrypoint Preview	15
Rich Headers	16
Data Directories	16
Sections	16
Resources	16
Imports	16
Version Infos	17

Network Behavior	17
UDP Packets	17
Code Manipulations	18
Statistics	18
Behavior	18
System Behavior	19
Analysis Process: loaddll32.exe PID: 6524 Parent PID: 5884	19
General	19
File Activities	19
Analysis Process: cmd.exe PID: 6536 Parent PID: 6524	19
General	19
File Activities	19
Analysis Process: rundll32.exe PID: 6548 Parent PID: 6536	19
General	19
Analysis Process: WerFault.exe PID: 6148 Parent PID: 6548	20
General	20
File Activities	20
File Created	20
File Deleted	20
File Written	21
Registry Activities	42
Key Created	42
Key Value Created	42
Disassembly	43
Code Analysis	43

Analysis Report 87324661_by_Libranalysis.dll

Overview

General Information

Sample Name:	87324661_by_Libranalysis.dll
Analysis ID:	413043
MD5:	873246614925ee..
SHA1:	b92a017964f94fa..
SHA256:	78bad82ee02304..
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...

Antivirus or Machine Learning detec...

Checks if the current process is bein...

Contains functionality to check if a d...

Contains functionality to query locale...

Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Classification

Startup

- System is w10x64
- loadll32.exe (PID: 6524 cmdline: loadll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
 - cmd.exe (PID: 6536 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 6548 cmdline: rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
 - WerFault.exe (PID: 6148 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6548 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 22202,
  "C2 list": [
    "203.114.109.124:443",
    "82.165.145.100:6601",
    "94.177.255.18:8172"
  ],
  "RC4 keys": [
    "BwjTiXD0nMT8wuL0LzuDMT1lwaJgYLnSPMpMch1H2fk8H",
    "q9klDr5IysNmmZqCx9jFzLSDl8TYcZm1jGiJKdnQSLg6QzqUnZo1jkSGDQVP1"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.426885605.0000000010001000.0000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

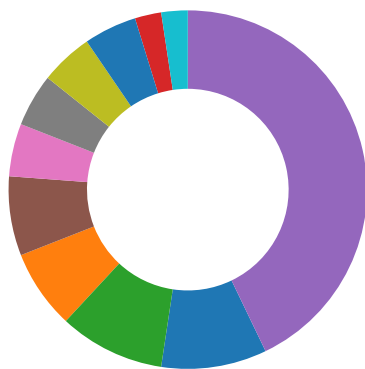
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



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



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Dridex unpacked file

Malware Analysis System Evasion:

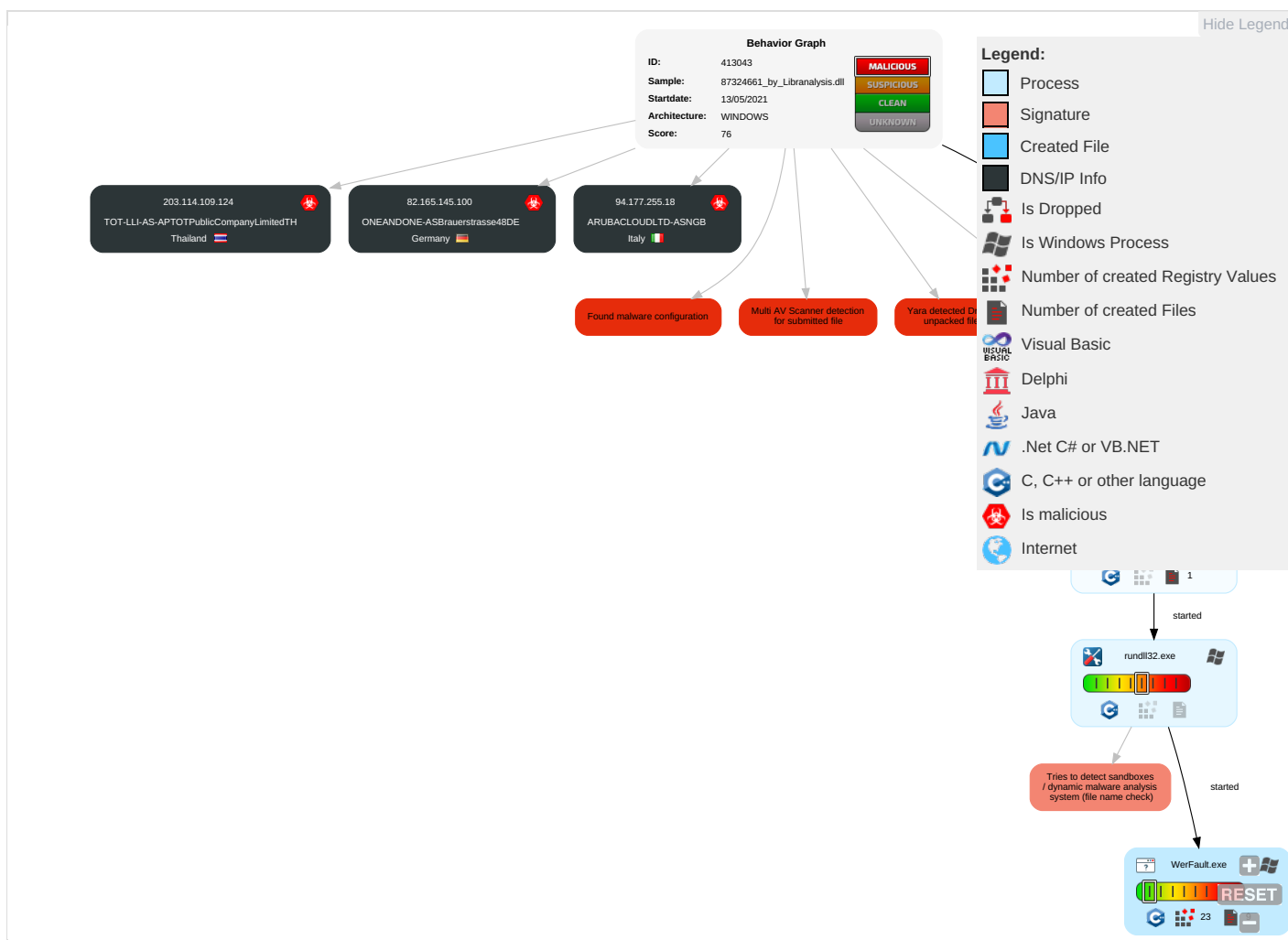


Tries to detect sandboxes / dynamic malware analysis system (file name check)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 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 3	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

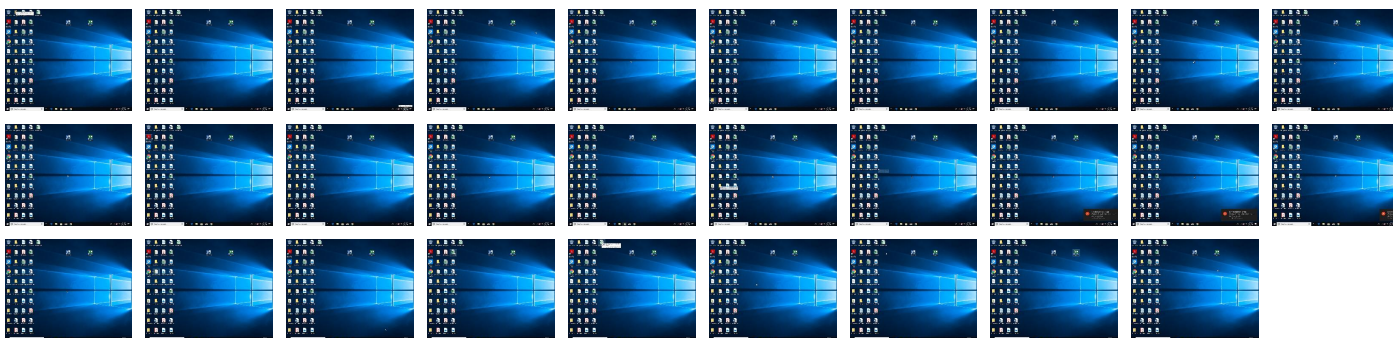
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
87324661_by_Libranalysis.dll	68%	ReversingLabs	Win32.InfoStealer.Dridex	
87324661_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.750000.1.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
2.2.rundll32.exe.a407fa.2.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://crl.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.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, 0000000C.00000000 2.423753260.0000000004E10000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	WerFault.exe, 0000000C.00000000 2.423753260.0000000004E10000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://ocsp.sectigo.com0	WerFault.exe, 0000000C.00000000 2.423753260.0000000004E10000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crt0#	WerFault.exe, 0000000C.00000000 2.423753260.0000000004E10000.0 0000002.00000001.sdmp, 8732466 1_by_Libranalysis.dll	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.177.255.18	unknown	Italy		199883	ARUBACLOUDLTD-ASNGB	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
82.165.145.100	unknown	Germany		8560	ONEANDONE-ASBraucherstrasse48DE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413043
Start date:	13.05.2021
Start time:	06:59:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	87324661_by_Libranalysis.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	28
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: 97.9% (good quality ratio 84.8%) • Quality average: 65.9% • Quality standard deviation: 35.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.177.255.18	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	
203.114.109.124	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
82.165.145.100	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBraucherstrasse48DE	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.165.145.100
	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
TOT-LLI-AS-APTOTPublicCompanyLimitedTH	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	• 203.114.10 9.124
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	e442 added_by_Libranalysis.dll	Get hash	malicious	Browse	203.114.10 9.124
	e442 added_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
	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
ARUBACLOUDLTD-ASNGB	042529de_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	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
	e442 added_by_Libranalysis.dll	Get hash	malicious	Browse	94.177.255.18
	e442 added_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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635da	
b\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635da hReport.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12688
Entropy (8bit):	3.7677347987958463
Encrypted:	false
SSDEEP:	192:8ciW0oXWYrYRHBUMX4jed+HYQR/u7sbS274ItWcb:/iQX4WBUZMX4jewb/u7sbX4ItWcb
MD5:	AAC8A45DA945FF7E9B3E3009BC82A638
SHA1:	E2058A747020021D038DF3690A3D0537C9B6DC6A
SHA-256:	A50F11E48321324EEA919B6F681A9E5355EECBCE25D899585E4482A90CC9D26
SHA-512:	4A583E25492E05A5EC8C98E3D8EA7A1A55B2794AEC4E3C5B7CA78EDAEEA15049214F4E146D5D5484003F04F8F0FA659C17325590BFD2CC5B78B11877D45AEA1
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.=1.3.2.6.5.3.8.8.0.8.1.2.6.6.5.1.0.0.....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.=1.3.2.6.5.3.8.8.0.9.0.0.6.3.3.4.5.1.....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.=0.2.9.e.f.f.2.0.-5.0.9.6.-4.d.a.d.-9.7.2.4.-5.e.c.2.6.e.5.c.4.b.e.7.....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.=8.e.5.0.a.1.7.d.-4.c.9.b.-4.a.8.c.-8.5.d.2.-6.9.6.e.1.a.7.3.e.a.8.d.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.9.9.4.-0.0.0.1.-0.0.1.7.-5.0.4.5.-a.6.6.0.0.0.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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.3.2.2.0.3.4.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\WER337E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:01:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	54272
Entropy (8bit):	2.070448844608849
Encrypted:	false
SSDEEP:	192:uj/lnODpnntmzj2t86q6GNvKpjY6l/UJ5USor0MbRdcnJP:lsDpnteS+FXvKpjNjSor0Mb0JJP
MD5:	01182E1499754A879B4269DD08B9D673
SHA1:	30DFDE41946D09686109DC88CAFEC1876D119D81
SHA-256:	081E1816369C3978B8D216B61A54F0F303E6CA9C003F34AB6931F148E0124DF7
SHA-512:	C1E6AB74339A9ED0AA5FAF3536DCBCD425988CC24DB48429F9D4C6B6966D6977EC22D0801DF3CBA379017896A4B8DFDA413CB3A8E0D0EDE1F249C7FD3F2836B
Malicious:	false
Reputation:	low
Preview:	MDMP.....51.`.....U.....B.....GenuineIntelW.....T.....1`.....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\WER4542.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):	3.6962715967639292
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNia46K6YFG6u7gmFTUYuS7Cprw89bUcsfecm:RrlsNi96K6YU6u7gmFTU/S+Uvfc
MD5:	DE25ACE16B1B443490D7790E4E37B50B
SHA1:	DBDB7A2429BBF4A4E0D1752D43FB44A10A39746C
SHA-256:	EE3163969C5762417EF8D097D9BEE0D903F9C7877EA119B0EFAC918ED790CAEC
SHA-512:	A05ABD1D69279D8282659F7BFF22AC4560FB61F4A427F9B4083C1E99184E88E66A1C76392688F372E277D937499AAEA087BF46A449BF98D3EAF3BB6DB9D0ED24
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.-16"?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>.1.0..0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d>.1.7.1.3.4.</B.u.i.l.d>.....<P.r.o.d.u.c.t>.(0.x.3.0).;. W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>.P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n>.....<B.u.i.l.d.S.t.r.i.n.g>.1.7.1.3.4..1...a.m.d.6.4.f.r.e...r.s.4...r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g>.....<R.e.v.i.s.i.o.n>.1.</R.e.v.i.s.i.o.n>.....<F.l.a.v.o.r>.M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r>.....<A.r.c.h.i.t.e.c.t.u.r.e>.X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D>.1.0.3.3.</L.C.I.D>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d>.6.5.4.8.</P.i.d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp.xml	
Size (bytes):	4663
Entropy (8bit):	4.4768227502647395
Encrypted:	false
SSDEEP:	48:cvlwSD8zsmJgtWI9acWSC8BV8fm8M4JCdsDNCFf+q8/KNFow4SrSyd:uITf8VVSNCJBNExNOwDWyd
MD5:	B31EF352DB23EC9479234D443D4B824C
SHA1:	9E4C0B04CF5087C8821BF8CB999DA7342AD2F44F
SHA-256:	A50448A29B2CBA57B5B6C559B106F30BE4E04BAF9BE3320F11FEE7B82768A726
SHA-512:	698573623B1EE765A326A897EDD8506B673E62B8008E0B72FB1B9599ED35EBCF849DA08219235AE45130AD2C7EC6C1A8C71ACFAEE4FF4ACA6F23EC712BD1527
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="987792" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.585730266072232
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	87324661_by_Libranalysis.dll
File size:	166856
MD5:	873246614925eed7eb818ffa6f785b75
SHA1:	b92a017964f94fa7cf2c77a95ea1095513c5431d
SHA256:	78bad82ee0230454a48cc41c1a951c304027ffc7d1b5d2c1b5bc4567db455109
SHA512:	92bca7ae32d548dfaaae3ae78de2f07d7dca1b43fc1039fd32a6a751662d4e3a8b7b2d56577d1c18b64d4b7d286f7025dfdc9787706c8cf100f339fc61e55013
SSDEEP:	3072:besl4+VdIY+01jb5SA5hg9PTEfPa1x+pq0KbuFicLiV:f4+VZQpt5hyPsa1ekiE9V
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.....zK.Rich0zK.....PE..L..

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x10023140
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F8E [Thu May 13 01:23:26 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a86a1220a8aaf2bed0594d018b59c83f

Authenticode Signature

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

Entrypoint Preview

Instruction

[illegible]

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

Rich Headers

Programming Language:	[RES] VS2012 UPD3 build 60610 [LNK] VS2005 build 50727 [EXP] VS2005 build 50727 [C] VS2012 UPD4 build 61030 [IMP] VS2013 UPD2 build 30501
-----------------------	---

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x222bc	0x22400	False	0.76244582573	data	7.58615299723	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x2a76	0x2c00	False	0.787819602273	SysEx File -	7.46416514998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x27000	0x3307	0x1800	False	0.76806640625	MMDF mailbox	7.41456160551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x3a0	0x400	False	0.423828125	data	3.05991849143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x230	0x400	False	0.4951171875	data	3.95131264834	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
ADVAPI32.dll	RegOverridePredefKey
CLUSAPI.dll	ClusterEnum
RASAPI32.dll	RasGetConnectionStatistics
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
OPENG32.dll	glTexSubImage1D
KERNEL32.dll	CloseHandle, LoadLibraryExA, OutputDebugStringA, CreateFileW, GetProfileSectionW, GetProfileSectionA, LoadLibraryW, OpenSemaphoreW
USER32.dll	TranslateMessage

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:00:41.893457890 CEST	49448	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:41.958832979 CEST	53	49448	8.8.8.8	192.168.2.6
May 13, 2021 07:00:41.963150978 CEST	60342	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:42.023719072 CEST	53	60342	8.8.8.8	192.168.2.6
May 13, 2021 07:00:43.009525061 CEST	61346	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:43.058197021 CEST	53	61346	8.8.8.8	192.168.2.6
May 13, 2021 07:00:44.206053972 CEST	51774	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:44.260063887 CEST	53	51774	8.8.8.8	192.168.2.6
May 13, 2021 07:00:45.117744923 CEST	56023	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:45.170605898 CEST	53	56023	8.8.8.8	192.168.2.6
May 13, 2021 07:00:45.248373032 CEST	58384	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:45.307473898 CEST	53	58384	8.8.8.8	192.168.2.6
May 13, 2021 07:00:46.041434050 CEST	60261	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:46.090190887 CEST	53	60261	8.8.8.8	192.168.2.6
May 13, 2021 07:00:47.266354084 CEST	56061	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:47.323142052 CEST	53	56061	8.8.8.8	192.168.2.6
May 13, 2021 07:00:48.705341101 CEST	58336	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:48.755635977 CEST	53	58336	8.8.8.8	192.168.2.6
May 13, 2021 07:00:49.926564932 CEST	53781	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:49.975981951 CEST	53	53781	8.8.8.8	192.168.2.6
May 13, 2021 07:00:53.525034904 CEST	54064	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:53.576534033 CEST	53	54064	8.8.8.8	192.168.2.6
May 13, 2021 07:00:54.519435883 CEST	52811	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:54.570425034 CEST	53	52811	8.8.8.8	192.168.2.6
May 13, 2021 07:00:55.774277925 CEST	55299	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:55.825789928 CEST	53	55299	8.8.8.8	192.168.2.6
May 13, 2021 07:00:56.775954962 CEST	63745	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:56.824548960 CEST	53	63745	8.8.8.8	192.168.2.6
May 13, 2021 07:00:57.673671961 CEST	50055	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:57.725392103 CEST	53	50055	8.8.8.8	192.168.2.6
May 13, 2021 07:00:59.181904078 CEST	61374	53	192.168.2.6	8.8.8.8
May 13, 2021 07:00:59.231870890 CEST	53	61374	8.8.8.8	192.168.2.6
May 13, 2021 07:01:00.127188921 CEST	50339	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:00.180078030 CEST	53	50339	8.8.8.8	192.168.2.6
May 13, 2021 07:01:01.056740999 CEST	63307	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:01.105460882 CEST	53	63307	8.8.8.8	192.168.2.6
May 13, 2021 07:01:02.336272001 CEST	49694	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:02.387949944 CEST	53	49694	8.8.8.8	192.168.2.6
May 13, 2021 07:01:07.225585938 CEST	54982	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:07.282747030 CEST	53	54982	8.8.8.8	192.168.2.6
May 13, 2021 07:01:17.919898033 CEST	50010	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:17.987698078 CEST	53	50010	8.8.8.8	192.168.2.6
May 13, 2021 07:01:28.756802082 CEST	63718	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:28.818485022 CEST	53	63718	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:01:31.659713030 CEST	62116	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:31.711353064 CEST	53	62116	8.8.8.8	192.168.2.6
May 13, 2021 07:01:37.370352030 CEST	63816	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:37.428669930 CEST	53	63816	8.8.8.8	192.168.2.6
May 13, 2021 07:01:49.818293095 CEST	55014	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:49.922055006 CEST	53	55014	8.8.8.8	192.168.2.6
May 13, 2021 07:01:50.534754992 CEST	62208	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:50.635096073 CEST	53	62208	8.8.8.8	192.168.2.6
May 13, 2021 07:01:51.189424038 CEST	57574	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:51.302253008 CEST	53	57574	8.8.8.8	192.168.2.6
May 13, 2021 07:01:51.741767883 CEST	51818	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:51.798705101 CEST	53	51818	8.8.8.8	192.168.2.6
May 13, 2021 07:01:51.885346889 CEST	56628	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:51.950364113 CEST	53	56628	8.8.8.8	192.168.2.6
May 13, 2021 07:01:52.747739077 CEST	60778	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:52.849320889 CEST	53	60778	8.8.8.8	192.168.2.6
May 13, 2021 07:01:53.450180054 CEST	53799	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:53.510077000 CEST	53	53799	8.8.8.8	192.168.2.6
May 13, 2021 07:01:54.064114094 CEST	54683	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:54.123277903 CEST	53	54683	8.8.8.8	192.168.2.6
May 13, 2021 07:01:55.586769104 CEST	59329	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:55.643933058 CEST	53	59329	8.8.8.8	192.168.2.6
May 13, 2021 07:01:55.981950998 CEST	64021	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:56.041843891 CEST	53	64021	8.8.8.8	192.168.2.6
May 13, 2021 07:01:56.744932890 CEST	56129	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:56.793565035 CEST	53	56129	8.8.8.8	192.168.2.6
May 13, 2021 07:01:57.478338003 CEST	58177	53	192.168.2.6	8.8.8.8
May 13, 2021 07:01:57.527640104 CEST	53	58177	8.8.8.8	192.168.2.6
May 13, 2021 07:02:21.019622087 CEST	50700	53	192.168.2.6	8.8.8.8
May 13, 2021 07:02:21.087264061 CEST	53	50700	8.8.8.8	192.168.2.6
May 13, 2021 07:02:26.954404116 CEST	54069	53	192.168.2.6	8.8.8.8
May 13, 2021 07:02:27.022258043 CEST	53	54069	8.8.8.8	192.168.2.6
May 13, 2021 07:02:29.071369886 CEST	61178	53	192.168.2.6	8.8.8.8
May 13, 2021 07:02:29.153188944 CEST	53	61178	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 6524 Parent PID: 5884

General

Start time:	07:00:48
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll'
Imagebase:	0x10000
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: 6536 Parent PID: 6524

General

Start time:	07:00:48
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1
Imagebase:	0x2a0000
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: 6548 Parent PID: 6536

General

Start time:	07:00:48
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\87324661_by_Libranalysis.dll',#1
Imagebase:	0xfa0000
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: 00000002.00000002.426885605.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6148 Parent PID: 6548

General

Start time:	07:01:19
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6548 -s 764
Imagebase:	0x2e0000
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	70131717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635dab	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635dab\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7012497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	success or wait	1	70124BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	success or wait	1	70124BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.tmp.xml	success or wait	1	70124BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A2.tmp.csv	success or wait	1	70124BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B8B.tmp.txt	success or wait	1	70124BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 35 31 9d 60 a4 05 12 00 00 00 00 00	MDMP.....51.`.....	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 b0 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 94 19 00 00 10 31 9d 60 07 00 00 00 11 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	U.....B..... ..GenuineIntelW.....T...1.`.....0.=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	...r.u.n.d.l.l.3.2...e.x.e...	success or wait	53	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 a0 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 70 74 02 00 00 00 00 00 c0 c4 02 00 00 00 00 7b 4c 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 25 72 03 00 00 00 00 00 3b 72 03 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 36 1b 00 00 00 00 00 33 c9 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 fd f8 04 00 00 00 00	..Ht....0...U..s@...&.....B.....B?.....#..... ..@A.....Zb.....pt..... {L.....%r.....;r6.....3..... @.....	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.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	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER337E.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 b6 34 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 e8 b5 00 00 15 00 00 00 ec 01 00 00 2c 1e 00 00 16 00 00 00 98 00 00 00 18 20 00 00	`..... ...4.....T.....8..... ...T.....`.....	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.l.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.5.4.8.</.P.i.d.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.I.I.3.2...e.x.e.</.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 39 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.6.9.3.3.<./U.p.t.i.m.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 39 00 33 00 35 00 39 00 38 00 37 00 32 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.>.1.2.9.3.5.9.8.7.2.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 39 00 33 00 35 00 31 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.9.3.5.1.6.8.0.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.6.0.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 36 00 31 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.6.1.7.6.0.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 36 00 31 00 37 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.6.1.7.6.0.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.1.8.6.6.4.8.<./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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 32 00 31 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>.3.2.1.4.4.<./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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 38 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>.3.1.8.7.2.<./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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 36 00 30 00 30 00 32 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.6.2.0.8.0.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 36 00 30 00 37 00 30 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.7.0.2.7.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 36 00 30 00 36 00 32 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e>.6.0.6.2.0.8.0.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d>.6.5.3.6.<./P.i.d>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	<.l.m.a.g.e.N.a.m.e>.c.m.d...e.x.e.<./l.m.a.g.e.N.a.m.e>.	success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 33 00 35 00 30 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>.3.7.3.5.0.<./U.p.t.i.m.e>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 34 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.>.1.1.2.4.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 32 00 37 00 33 00 36 00 30 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.>.3.7.2.7.3.6.0.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 30 00 34 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.0.4.9.6.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 34 00 39 00 34 00 34 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.9.4.4.6.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.0.0.3.8.4.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 34 00 39 00 34 00 34 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.4.9.4.4.6.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.I.I.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 67 00 74 00 62 00 71 00 77 00 66 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.>.g.t.b.q.w.f.,.l.n.c...</.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 67 00 74 00 62 00 71 00 77 00 66 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.>.g.t.b.q.w.f.7,,1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 38 00 30 00 36 00 39 00 38 00 36 00 39 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.8.0.6.9.8.6.9.6.</.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 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.<./F.l.a.g.s.>.	success or wait	3	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 34 00 3a 00 30 00 31 00 3a 00 32 00 36 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.1.4.:.0.1.: 2.6.Z.">.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 35 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 34 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 32 00 38 00 39 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 39 00 38 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.l.d.= ".3.5.5". .P.I.D.= ".6.5.4.8". .U.p.t.i.m.e.M.S.= ".2.8.9.8.4". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.8.9.8.4". .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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 32 00 39 00 65 00 66 00 66 00 32 00 30 00 2d 00 35 00 30 00 39 00 36 00 2d 00 34 00 64 00 61 00 64 00 2d 00 39 00 37 00 32 00 34 00 2d 00 35 00 65 00 63 00 32 00 36 00 65 00 35 00 63 00 34 00 62 00 65 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.2.9.e.f.f.2.0.-.5.0.9.6.-.4.d.a.d.-.9.7.2.4.-.5.e.c.2.6.e.5.c.4.b.e.7.<./G.u.i.d.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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 34 00 3a 00 30 00 31 00 3a 00 32 00 36 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.1.4.:.0.1.:.2.6.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4542.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	7012497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER47A4.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"?>.. ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635dab\Report.wer	unknown	2	ff fe	..	success or wait	1	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635dab\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	7012497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_8312e17df74c6535839b6a3ab171c47136d6e399_82810a17_18635dab\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 36 00 32 00 34 00 39 00 31 00 38 00 39 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.= -2.0.6.2.4.9.1.8.9.2.	success or wait	1	7012497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701436BF	unknown
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701436BF	unknown
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	success or wait	1	701436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70141FB2	RegCreateKeyExW
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701243D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	701436BF	unknown
\REGISTRYA\{99c1cd71-11eb-c0d6-baac-59d8783908a6}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	701436BF	unknown

